NT Bestyrelse (Møde i NT's bestyrelse)

16-02-2024 09:00 - 12:00

J. F. Kennedys Plads 1T, 9000 Aalborg, mødelokale 10 og 11

Information: Der er mulighed for frokost efter mødet.

Indhold

9. februar 2024

1. Planlagte salgs- og kampagnetiltag i 2024

I NT's administration har vi fortsat stort fokus på at få kunderne tilbage i den kollektive trafik.

I 2024 igangsættes forskellige initiativer ud mod forskellige målgrupper og med forskelligt fokus. På mødet vil salgs- og kampagnetiltagene i 2024 blive præsenteret.

Det indstilles,

- at orienteringen tages til efterretning.

9. februar 2024

2. Tema om samkørsel

I Danmark har vi en dårlig kapacitetsudnyttelse af private biler. På alle bilrejser sidder der kun 1,4 person i bilerne generelt. I myldretiden er tallet endnu lavere, da der her kun sidder 1,08 person i hver bil. Vejdirektoratet har beregnet, at der hver dag er 4 mio. ledige sæder i myldretiden i Danmark.

Antallet at biler stiger, og der er derfor et stort potentiale i samkørsel i Danmark. På daglig basis har DTU har beregnet, at hvis blot 10 % af bilisterne i landdistrikterne medtager én passager, vil det svare til en fordobling af den kollektive trafik i landdistrikterne.

"Vi rejser sammen" er et væsentligt element i NT's mobilitetsplan, fordi det at rejse sammen understøtter den kollektive trafik og også har den fordel, at det bidrager til et bedre klima og mindre trængsel på vejene.

I NT har vi fokus på nye mobilitetsformer, fordi de i kombination med den kollektive trafik kan give endnu flere rejsemuligheder til nordjyderne og også udvide rækkevidden af den kollektive trafik. Produkter som Plustur giver hovednettet større rækkevidde og sikrer, at flere får gavn af et styrket hovednet. Ligesom Plustur kan nye mobilitetsformer bidrage til en styrket mobilitet, når det kombineres med den kollektive trafik.

NT har derfor etableret et partnerskab med en udbyder af samkørsel. Pilotprojektet skal afdække potentialet for samkørsel med særligt fokus på landdistrikterne. I landområder, hvor serviceniveauet i den kollektive trafik er lavt, er det ambitionen at udvikle et koncept for samkørsels-korridorer, der forbinder landområder med de større byer, hvor man kan komme videre med ekspresbusser og tog i NT's hovednet.

Projektet om samkørsel i Nordjylland har fået en del positiv opmærksomhed fra forskellig side, og der er også positive udmeldinger fra bl.a. transportministeren om at styrke incitamenterne til samkørsel. Samkørsel er i dag reguleret. Og yderligere liberalisering af området, vil kræve ændringer i både taxiloven, skatteloven og lov om trafikselskaber.

På bestyrelsesmødet gives en status for samkørsel i Nordjylland og konceptet for samkørselsruter samt overvejelser om, hvordan NT på længere sigt kan integrere og finansiere samkørslen som en del af den kollektive trafik i Nordjylland.

Det indstilles,

- at orienteringen tages til efterretning.

9. februar 2024

3. Audit vedr. GDPR

NT's eksterne DPO, DPO-Danmark, har som en del af deres lovpligtige opgave som NT's DPO i 4. kvartal 2023 gennemført et årligt tilsyn vedrørende vores GDPR-compliance. Resultaterne fra tilsynet er afrapporteret i en rapport, hvori DPO-Danmark har givet en status på niveauet for GDPR-compliance hos NT.

I NT bruger vi rapporten aktivt som et redskab i vores løbende indsats for at sikre en korrekt håndtering af personoplysninger. Vi bruger eksempelvis rapporten:

- Som et værktøj til at øge opmærksomhedsniveauet i organisationen omkring GDPR.
- Som et redskab til at få implementeret nye/supplerende GDPR-aktiviteter.
- Som et grundlag til at prioritere handlinger/aktiviteter.

Samlet set viser resultaterne fra tilsynet, at vi i NT har et GDPR-compliance niveau 3 eller 4 på langt hovedparten af kontrolpunkterne i den gennemførte audit. For en mindre del (18 %) var scoren 2. En score på 4 er det højest mulige. Der er i 2023-auditen ikke nogen af de gennemførte kontroller, der har resulteret i det laveste compliance niveau 1 (kritisk mangel).

Sammenholdt med den audit, der blev gennemført i 2022, er vi i løbet af 2023 lykkedes med at få implementeret relevante tiltag på områderne for gennemsigtighed og kontrol med personoplysninger, sikring af persondata samt tekniske og organisatoriske foranstaltninger. Der er med dette taget nogle store skridt i retningen af at opnå fuld GDPR-compliance.

Sammenfattende for den gennemførte audit er konklusionen fra DPO-Danmark: "*NT's gennemsnitlige GDPR-compliance niveau var på 3,5 på tidspunktet for tilsynet i 2023, i forhold til sidste års GDPR-compliance niveau på 2,8, hvilket illustrerer en flot indsats. Resultatet afspejler, at organisationen generelt har et godt compliance niveau i forhold til alle tilsynsområder, mens der samtidigt er plads til forbedring i forhold til flere af kontrollerne*."

På bestyrelsesmødet gennemgås, hvordan NT arbejder med sikkerhedskultur og awareness samt hovedpunkterne i den seneste audit og de elementer, der i en kommende handleplan, skal understøtte det vedvarende arbejde med at hæve compliance niveauet.

Den fulde auditrapport fra NT's DPO fremgår af vedlagte.

Det indstilles,

- at orienteringen tages til efterretning.

Bilag

Bilag 3 – GDPR compliancerapport - Nordjyllands Trafikselskab 2023.

GDPR compliancerapport
Nordjyllands Trafikselskab
Oktober 2023

DPO-Danmark ApS | www.DPO-Danmark.dk
Højbro Plads 10, 1200 København K
CVR: 30 98 85 31 | Tlf. 77 34 17 34

Indholdsfortegnelse

Introduktion

DPO-Danmark har i 4. kvartal 2023 gennemført et årligt tilsyn vedrørende GDPR-compliance hos Nordjyllands Trafikselskab.

Resultaterne fra tilsynet afrapporteres i denne rapport til ledelsen. Rapporten giver en status på niveauet for GDPR-compliance hos Nordjyllands Trafikselskab.

Rapporten kan samtidig bruges af Nordjyllands Trafikselskab som et benchmarking værktøj til over tid at øge niveauet for GDPR-compliance, som et redskab til arbejdet med implementering af GDPR i bund og/eller som et grundlag til at iværksætte prioriteret afhjælpning.

Tilsynet udføres som en del af DPO-Danmarks lovpligtige opgave som DPO for Nordjyllands Trafikselskab med at føre tilsyn med GDPR-compliance hos Nordjyllands Trafikselskab.

Rapporten indeholder følgende afsnit: vurderingsskala, tilsynstemaer og kontroller, ledelsesresume samt afsluttende bemærkninger. Rapportens bilag 1 indeholder læsevejledning, skema med kontroller, vurderinger, anbefalinger og prioriteringsforslag. Rapportens bilag 2 indeholder oversigt over årets handlinger.

Vurderingsskala

DPO Danmarks tilsyn vedrørende databeskyttelse hos Nordjyllands Trafikselskab er baseret på en 4-trins skala, hvor 1 er lavest og 4 er højeste complianceniveau.

Niveau 1-3 indikerer manglende GDPR-compliance, hvor niveau 1 er kritisk mangel, niveau 2 er væsentlig mangel og niveau 3 er mindre væsentlig mangel. Niveau 4 indikerer GDPR-compliance.

Nordjyllands Trafikselskab bør stræbe efter at være på niveau 3 eller højere.
På niveau 1-2 er der risiko for alvorlig kritik og bøder fra Datatilsynet i tilfælde af tilsyn. På niveau 3 er der risiko for kritik fra Datatilsynet i tilfælde af tilsyn.

Compliance niveau		Beskrivelse	Prioritet
1		**Kritisk mangel** Anvendes ved forhold eller risici, der anses for kritiske. Et *forhold* anses som kritisk, når der er tale om en alvorlig mangel i strid med databeskyttelsesretlige krav. En *risiko* anses for kritisk, hvis der er en høj grad af sandsynlig risiko for de registreredes rettigheder og frihedsrettigheder. Prioritet 1 markeringer (P1) rapporteres til ledelsen med anbefaling om at afhjælpe forholdet straks.	**P1**
2		**Væsentlig mangel** Anvendes ved forhold eller risici, der anses for væsentlige. Et *forhold* anses for væsentligt, når der er tale om en mangel i strid med databeskyttelsesretlige regler. En *risiko* anses for væsentlig, hvis der er middel grad af sandsynlig risiko for de registreredes rettigheder og frihedsrettigheder. Prioritet 2 markeringer (P2) rapporteres til ledelsen med anbefaling om, at ledelsen afhjælper forholdet.	**P2**
3		**Mindre væsentlig mangel** Anvendes ved forhold eller risici, der anses for mindre væsentlige. Et forhold anses for mindre væsentligt, når det er tale om en uvæsentlig mangel i strid med databeskyttelsesretlige regler. En risiko anses for mindre væsentlig, hvis der er en lille grad af sandsynlig risiko for de registreredes rettigheder og frihedsrettigheder. Prioritet 3 markeringer (P3) rapporteres kun til ledelsen som opmærksomhedspunkter, men med en anbefaling til ledelsen om at tage stilling til, om forholdet giver anledning til yderligere opfølgning.	**P3**
4		**Overholdelse** Databeskyttelsesretlige krav overholdes, med mulighed for forbedring i konkrete tilfælde.	**N/A**

Tilsynstemaer og kontroller

DPO Danmarks tilsyn dækker fire tilsynstemaer med tilhørende kontroller, som afspejler krav efter GDPR eller på anden måde har betydning for beskyttelse af persondata.

A. Gennemsigtighed og kontrol med persondata

- A1. Behandlingshjemmel
- A2. Samtykke
- A3. Sletning af persondata
- A4. Oplysningspligt
- A5. Registreredes rettigheder
- A6. Fortegnelse
- A7. Overførsel til usikre tredjelande

B. Sikring af databeskyttelse

- B1. Privacy by design og default
- B2. Databehandleraftaler
- B3. Tilsyn med databehandlere
- B4. Risikovurderinger
- B5. Håndtering af brud på persondatasikkerhed
- B6. Konsekvensanalyse (DPIA)

C. Tekniske foranstaltninger

- C1. Antivirus
- C2. Firewall
- C3. Segmentering af netværk
- C4. Adgangsstyring
- C5. Logning
- C6. Systemovervågning
- C7. Kryptering af harddisk og filsystem
- C8. Kryptering via internettet
- C9. Sårbarheder og penetrationstests
- C10. Opdateringer og patches
- C11. To-faktor autentifikation
- C12. Backup

D. Organisatoriske foranstaltninger (governance)

- D1. Informationssikkerhedspolitik
- D2. Roller og ansvar
- D3. Ledelsesforankring
- D4. Årshjul
- D5. Uddannelse og awareness
- D6. Business Recovery Plan
- D7. Disaster Recovery Plan
- D8. Fysisk sikkerhed

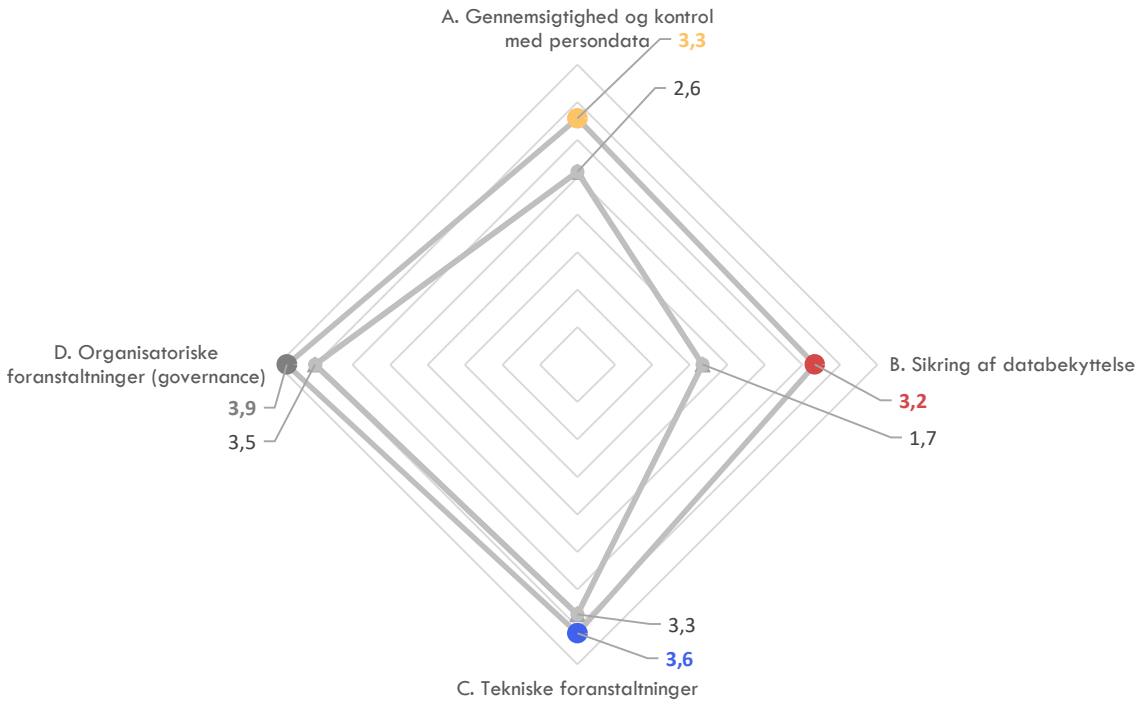
Ledelsesresumé

Samlet set viser resultaterne fra tilsynet, at organisationen har et GDPR-complianceniveau på 3 eller 4 for så vidt angår 82% af kontrollerne. Organisationen har implementeret relevante tiltag på områderne for gennemsigtighed og kontrol med personoplysninger, sikring af persondata samt tekniske og organisatoriske foranstaltninger (tilsynstema A, B, C og D), hvilket er meget positivt. Resultaterne viser, at organisationen i forhold til 18% af kontroller, som vedrører centrale krav efter GDPR, dog har et lavere complianceniveau på 2. Det skal dog positivt bemærkes, at organisationen ikke har nogen kontroller på det laveste compliance niveau 1. Områderne hvor organisationen har et lavt GDPR complianceniveau gælder dels i forhold til området for gennemsigtighed og kontrol med personoplysninger (tilsynstema A) og området for sikring af databeskyttelse (tilsynstema B) samt området for tekniske foranstaltninger (tilsynstema C). På tidspunktet for tilsynet var der således i forhold til de pågældende områder nogle centrale krav efter GDPR, som organisationen ikke efterlevede. Dette medfører risiko for manglende beskyttelse af de registreredes rettigheder og frihedsrettigheder, herunder risiko for kritik eller bøder fra Datatilsynet, hvis tilsynet skulle undersøge organisationens overholdelse af de pågældende GDPR-krav.

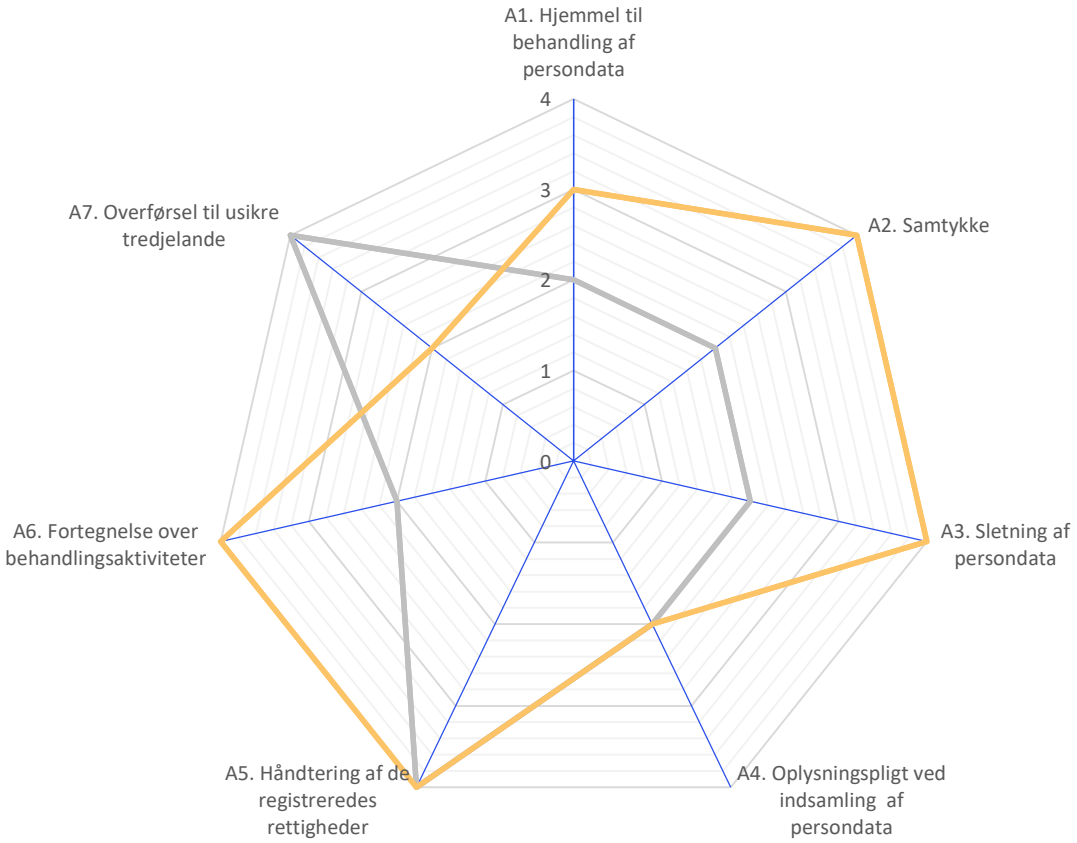
Organisationens gennemsnitlige GDPR-complianceniveau var på 3,5 på tidspunktet for tilsynet i 2023, i forhold til sidste års GDPR-complianceniveau på 2,8, hvilket illustrerer en flot indsats. Resultatet afspejler, at organisationen generelt har et godt complianceniveau i forhold til alle tilsynsområder, mens der samtidigt er plads til forbedring i forhold til flere af kontrollerne (se nedenfor).

Gennemsnit på baggrund af kontroltemaer

I den følgende model præsenteres gennemsnitsresultaterne for tilsynet, fordelt på kontroltemaerne. De fire scorer udgør gennemsnittet af organisationens samlede score indenfor det pågældende kontroltema.

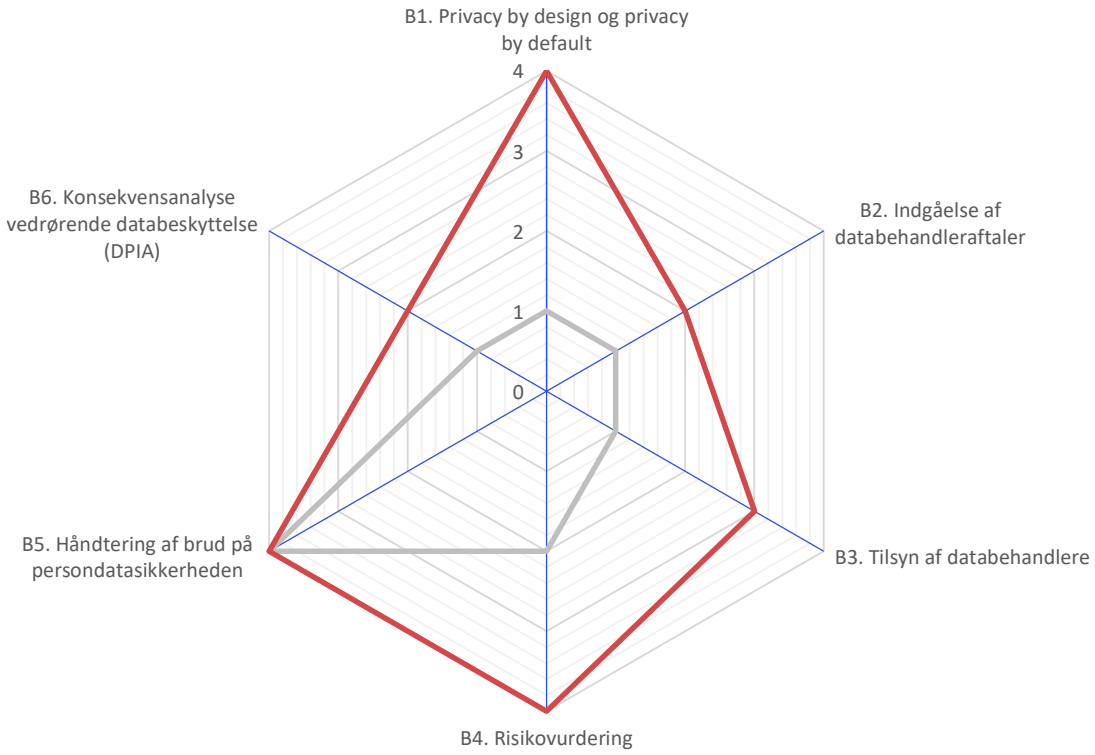


Tilsynstema A - Gennemsigtighed og kontrol med personoplysninger



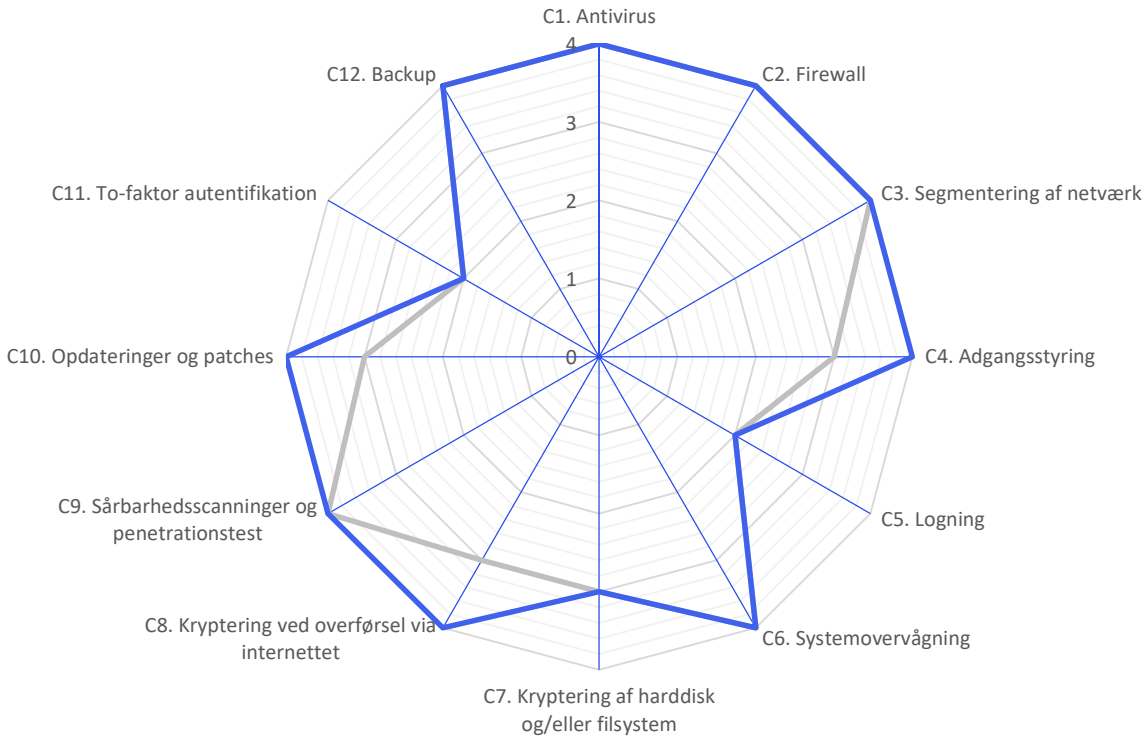
På dette område udgør gennemsnitsniveauet for compliance 3,3, i forhold til sidste år, som lå på 2,6. Organisationen har godt styr på sletning af persondata, håndtering af de registreredes rettigheder samt på at føre fortegnelse over organisationens behandlingsaktiviteter. Det trækker dog ned, at identificeret behandlingshjemmel i organisationens fortegnelser fortsat mangler nogle steder. Derudover trækker det ned, der ikke foreligger en skriftlig procedure for de behandlinger som kræver, at der bliver indhentet et gyldigt samtykke. Det trækker herudover ned, at organisationen ikke i alle tilfælde ses, at organisationen ikke efterlever oplysningspligten over for flexkunder i forbindelse med indsamling af persondata om flexkunder fra tredjemand (regionen og kommuner) samt, at organisationen ikke har sikret, der er fundet et overførselsgrundlag ved overførsel af personoplysninger til usikre tredjelande.

Tilsynstema B - Sikring af databeskyttelse



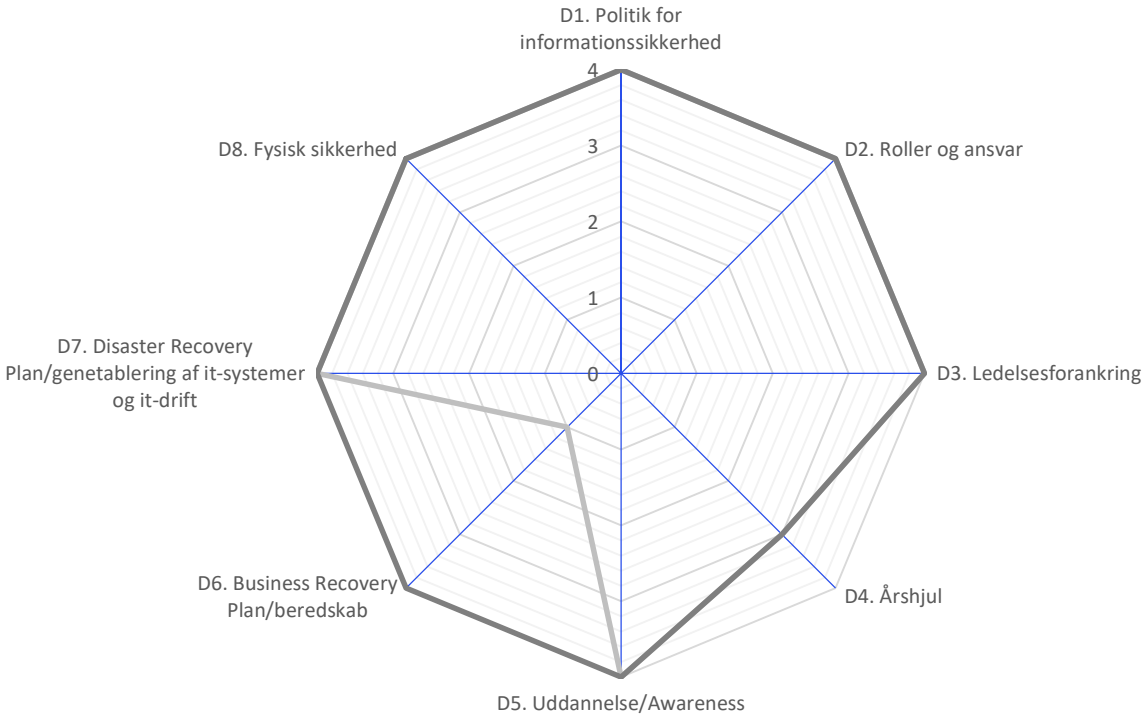
På området her udgør gennemsnitsniveauet for compliance 3,2, i forhold til sidste år, som lå på 1,7. Organisationens complianceniveau ligger gennemsnitligt godt, men en del af kontroller på området trækker complianceniveauet ned. De kontroller organisationen klarer sig særligt godt på, er området for privacy by design og privacy by default, etableringen af en risikovurdering, der i et tilstrækkeligt omfang identificerer trusler og tager højde for alle relevante parametre efter GDPR i forbindelse med vurdering af risici for de registreredes rettigheder og frihedsrettigheder samt området for håndtering af brud på persondatasikkerheden. Det trækker complianceniveauet ned, at organisationen ikke har indgået databehandleraftaler med alle leverandører, som behandler persondata for organisationen, ligesom det trækker ned, at organisationen ikke på tidspunktet for tilsyn har ført passende tilsyn af databehandlere. Dog skal det bemærkes, at organisationen har planlagt tilsyn ud fra et konkret tilsynskoncept med hver enkelt databehandler. Det trækker foruden ned, at organisationen ikke har etableret en formaliseret proces, som sikrer, at organisationen kan identificere høj risiko behandlinger og gennemføre en konsekvensanalyse forinden behandling, hvis dette er påkrævet efter GDPR. Kontrollerne der omhandler indgåelse af databehandleraftaler og tilsyn med databehandlere, samt identificering af høj risiko behandlinger og gennemførelse af konsekvensanalyse ved påkrav herom er centrale GDPR krav, som har til formål at sikre, at der er et passende sikkerhedsniveau for de registrerede.

Tilsynstema C - Tekniske foranstaltninger



På dette område er gennemsnitsniveauet for compliance 3,6, i forhold til sidste år, som lå på 3,3. Organisationen har implementeret mange relevante tekniske foranstaltninger, som beskytter informationssikkerhed og persondata. Organisationens complianceniveau ligger generelt højt på området. Det trækker dog ned, at organisations logfiler ikke bliver opsamlet på en særskilt logserver, samt at organisationen ikke har en overordnet logningsstrategi. Desuden trækker det organisationens GDPR-complianceniveau ned, at kryptering ikke er slået til på system-niveau. En yderligere kontrol, der trækker niveauet ned er, at logfiler ikke opbevares på særskilt logserver, herunder at der ikke anvendes traditionel to-faktor autentifikation til systemer og databaser.

Tilsynstema D - Organisatoriske foranstaltninger/governance



På området for organisatoriske foranstaltninger udgør gennemsnitsniveauet for compliance 3,9, i forhold til sidste år, som lå på 3,5. Organisationen har implementeret mange relevante organisatoriske foranstaltninger, som beskytter informationssikkerhed og persondata. Organisationens GDPR-complianceniveau ligger generelt meget højt på området, hvilket indikerer, at organisationen har lagt et betydeligt arbejde i at sikre overholdelsen af de organisatoriske foranstaltninger. Det trækker dog ned, at organisationen ikke har etableret et årshjul, som understøtter opgaver vedrørende væsentlige politikker og procedurer, der understøtter efterlevelsen af databeskyttelse og informationssikkerhed.

Anbefalinger

Det er DPO Danmarks anbefaling at organisationen, som første prioritet, øger complianceniveauet i forhold til følgende kontroller:

Prioritet - P2

P2	A4. Oplysningspligt ved indsamling af persondata
P2	A7. Overførsel til usikre tredjelande
P2	B2. Indgåelse af databehandleraftaler
P2	B6. Konsekvensanalyse vedrørende databeskyttelse (DPIA)
P2	C5. Logning
P2	C11. To-faktor autentifikation

Det er derudover DPO Danmarks anbefaling, at organisationen, som anden prioritet, øger complianceniveauet i forhold til følgende kontroller:

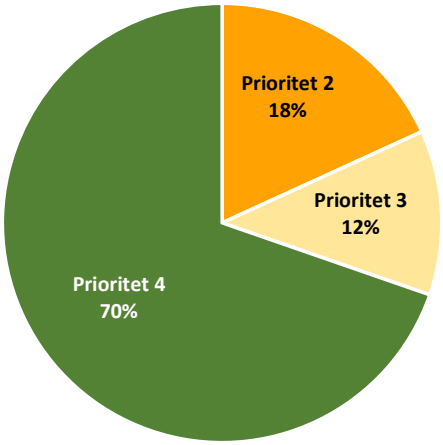
Prioritet - P3

P3	A1. Hjemmel til behandling af persondata
P3	B3. Tilsyn af databehandlere
P3	C7. Kryptering af harddisk og/eller filsystem
P3	D4. Årshjul

Der henvises i øvrigt til DPO Danmarks konkrete vurderinger og anbefalinger i forhold til de enkelte kontroller i bilag 1A-1D.

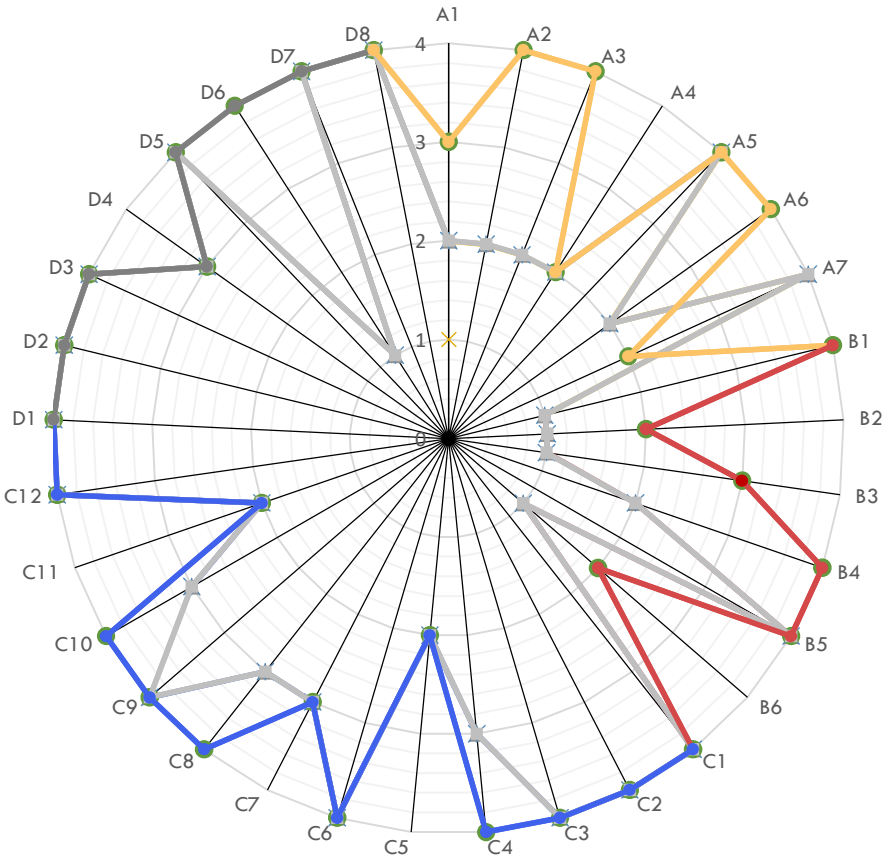
Oversigt over fordeling af prioriteter

Cirkeldiagrammet repræsenterer fordelingen af de forskellige prioteter på tværs af kontrollerne.



Oversigt over alle kontroller

I nedenstående model præsenteres de samlede resultater fra tilsynet med kontrollerne. Samtlige af organisationens scorer for de udvalgte kontroller uddybes i vurderingsskalaen på side 3. En uddybning af kontrollernes score findes i bilag 1A-1D.



Afsluttende bemærkninger og næste tilsyn

Det næste DPO tilsyn bliver udført i 2024.

Indeværende rapport er d. 25. oktober 2023 udarbejdet af

_____

Michael Nielsen
Partner, Direktør
DPO Danmark ApS

og

_____

Isabella Westh
Compliancekonsulent, cand.jur.
DPO Danmark ApS

og

_____

Nadia Bayrampour
Compliancekonsulent, cand.merc.(jur.)
DPO Danmark ApS

Bilag 1: Kontroller og læsevejledning til disse

Felt	Beskrivelse
Compliancemål	Kontrollens mål. Det, som skal være opfyldt for at efterleve kontrollen/være i compliance.
Complianceniveau	Markering af kundens aktuelle complianceniveau (score) baseret på en konkret vurdering af niveauet for efterlevelse af kontrollen.
Prioritet	Markering af prioritet for afhjælpning afhængig af kundens aktuelle complianceniveau.
Undersøgelse	Handlinger, som DPO'en har foretaget for at undersøge complianceniveauet for kontrollen. "Undersøgelse" betyder, at DPO'en har stillet spørgsmål til relevant personale hos kunden om, hvordan kontrollen efterleves. "Inspicering" betyder, at DPO'en har gennemgået materiale fra kunden, som indeholder information om efterlevelse af kontrollen. "Observation" betyder, at DPO'en har observeret, hvordan kontrollen efterleves hos kunden.
Vurdering	DPO'ens konkrete vurdering af niveauet for efterlevelse af kontrollen hos kunden.
Anbefaling	DPO'ens konkrete anbefaling til kunden.

Bilag 1A: Vurderingsgrundlag og anbefalinger for gennemsigtighed og kontrol med personoplysninger

A. Gennemsigtighed og kontrol med persondata

A1. Hjemmel til behandling af persondata

Der må kun behandles persondata, hvis der er hjemmel til behandling af persondata (GDPR artikel 6 og 9)

Compliancemål	Compliancenivau		Prioritet
Der er identificeret hjemmel til behandling af persondata.	3		P3

Undersøgelse

Vi har undersøgt, om der er en opdateret oversigt over behandlingshjemmel for enhver behandling af persondata.

Vi har inspiceret, om der foreligger en dokumenteret oversigt over behandlingshjemmel, om denne er opdateret, og om behandlingshjemmel forekommer korrekt.

Vurdering

Organisationen har opdateret sine fortegnelser siden sidste tilsyn, hvilket viser et flot resultat. Det vurderes, at organisationen fører en dokumenteret oversigt over behandlingshjemmel.

Organisationen er på tidspunktet for tilsynet nået langt, men stadig ikke helt i mål med deres identificering af behandlingshjemmel for alle behandlingsaktiviteter.

Anbefaling

Vi anbefaler organisationen at gennemgå alle behandlingsaktiviteter og identificere behandlingshjemmel for de aktiviteter, der på nuværende tidspunkt mangler anførelse af hjemmel efter GDPR og databeskyttelsesloven.

A2. Samtykke

Behandling af persondata på grundlag af samtykke skal altid være baseret på gyldigt samtykke fra de personer, som er genstand for behandlingen (de registrerede) (GDPR artikel 4, nr. 11 og artikel 7).

Compliancemål	Complianceniveau	Prioritet
Der behandles kun persondata på baggrund af gyldigt samtykke fra de registrerede.	4 ✓	n/a

Undersøgelse

Vi har undersøgt, om der foreligger skriftlig procedure, som sikrer, at der indhentes gyldigt samtykke fra de registrerede, forinden behandling af persondata på grundlag af samtykke.

Vi har inspiceret for en udvalgt behandlingsaktivitet, at indhentet samtykke fra de registrerede forekommer gyldigt.

Vurdering

Det vurderes, at organisationen har arbejdet godt med opdatering af deres skabeloner for samtykkeerklæringer og etablering af skriftlige procedurer siden sidste tilsyn.

Anbefaling

Ingen.

A3. Sletning af persondata

Persondata må ikke opbevares i et længere tidsrum end det, der er nødvendigt til de formål, hvortil de pågældende persondata behandles. Det vil med andre ord sige, at man ikke må behandle persondata længere end nødvendigt. Herefter skal oplysninger slettes eller anonymiseres (GDPR artikel 5)

Compliancemål	Complianceniveau	Prioritet
Persondata opbevares ikke længere end nødvendigt.	4 ✓	n/a

Undersøgelse

Vi har undersøgt, om der foreligger opdateret skriftlig procedure, som sikrer, at persondata slettes.

Vi har inspiceret, at den skriftlige procedure er opdateret og forekommer tilstrækkelig for sletning af persondata.

Vurdering

Organisationen har gjort et godt stykke arbejde. Compliancemålet vurderes, på det foreliggende grundlag, at være opfyldt, men der kan være mulighed for forbedring i konkrete tilfælde.

Anbefaling

Ingen.

A4. Oplysningspligt ved indsamling af persondata

Når der indsamles persondata om personer, som er genstand for behandling (de registrerede), skal der udleveres skriftlig information om behandlingen til de registrerede. Der skal udleveres information om: Navn på og kontaktoplysninger for den dataansvarlige og databeskyttelsesrådgiveren, formål og retsgrundlag for behandling, typer af persondata (kun artikel 14), kilder hvorfra persondata hidrører (kun artikel 14), kategorier af modtagere som oplysningerne videregives til, herunder GDPR-rettighederne for de registrerede. (GDPR artikel 13-14)

Compliancemål	Complianceniveau	Prioritet
Der udleveres tilstrækkelig skriftlig information om behandlingen til de registrerede ved indsamling af persondata.	2	P2

Undersøgelse

Vi har undersøgt, om der foreligger opdateret skriftlig procedure, som sikrer, at der udleveres information om behandlingen til de registrerede ved indsamling af persondata.

Vi har, for en udvalgt behandlingsaktivitet inspiceret, at udleveret information til de registrerede forekommer i overensstemmelse med minimumskravene efter GDPR artikel 13-14.

Vurdering

Generelt vurderes organisationen at udlevere information om behandling af persondata via deres hjemmeside. For behandlinger, hvori der indgår CPR-nummer, har organisationen opdateret deres privatlivspolitikker med en henvisning til Databeskyttelseslovens § 11, hvilket er positivt.

Det vurderes desuden, at organisationen på tidspunktet for tilsynet fortsat ikke efterlever oplysningspligten over for flexkunder i forbindelse med, at organisationen modtager persondata om flekskunder fra regionen og kommuner (tredjemand), da organisationen ikke udleverer information til flexkunder som beskrevet i artikel 14 i GDPR senest 30 efter modtagelsen af persondata fra tredjemand.

Organisationen har ikke udarbejdet en skriftlig procedure, som sikrer efterlevelse af oplysningspligten i forhold til alle kanaler, hvorigennem organisationen indsamler persondata.

Anbefaling

Det anbefales fortsat organisationen at sikre efterlevelse af oplysningspligten over for flexkunder senest 30 dage efter modtagelse af persondata fra tredjemand.

Det anbefales desuden, at udarbejde skriftlige procedurer, som sikrer efterlevelse af oplysningspligten, herunder som identificerer alle kanaler, hvorigennem organisationen indsamler persondata fra registrerede.

A5. Håndtering af de registreredes rettigheder

De personer, som er genstand for behandling af persondata (de registrerede), har en række rettigheder efter GDPR fx ret til indsigt i persondata, ret til berigtigelse af forkert persondata, ret til at anmode om sletning af persondata, og ret til at gøre indsigelse mod behandling af persondata. Henvendelser fra de registrerede, som gør brug af deres GDPR-rettigheder, skal håndteres hurtigst muligt og senest inden for en 30-dages frist. (GDPR artikel 12 og artikel 15-22).

Compliancemål	Complianceniveau	Prioritet
De registreredes rettigheder kan håndteres	4 ✓	n/a

Undersøgelse

Vi har undersøgt, om der foreligger skriftlig procedure, som sikrer, at henvendelser fra de registrerede kan håndteres.

Vi har inspiceret, at skriftlig procedure er opdateret og forekommer tilstrækkelig for håndtering af de registreredes rettigheder.

Vurdering

Organisationen har gjort et godt stykke arbejde. Compliancemålet vurderes, på det foreliggende grundlag, at være opfyldt, men der kan være mulighed for forbedring i konkrete tilfælde.

Anbefaling

Ingen.

A6. Fortegnelse over behandlingsaktiviteter

Der skal føres en skriftlig og elektronisk fortegnelse (oversigt) over alle behandlinger af persondata (behandlingsaktiviteter). Fortegnelsen skal bl.a. indeholde følgende oplysninger: Navn på og kontaktoplysninger for den dataansvarlige og databeskyttelsesrådgiveren, formålene med behandlingerne af persondata, beskrivelse af kategorierne af registrerede og typer af persondata, herunder kategorier af modtagere, som persondata videregives til. (GDPR artikel 30).

Compliancemål	Complianceniveau	Prioritet
Der føres en fortegnelse over alle behandlingsaktiviteter.	4 ✓	n/a

Undersøgelse

Vi har undersøgt, om der føres en opdateret fortegnelse over alle behandlingsaktiviteter.

Vi har inspiceret, at fortegnelsen er opdateret og forekommer i overensstemmelse med minimumskravene efter GDPR artikel 30.

Vurdering

Organisationen har gjort et godt stykke arbejde. Compliancemålet vurderes, på det foreliggende grundlag, at være opfyldt, men der kan være mulighed for forbedring i konkrete tilfælde.

Anbefaling

Ingen.

A7. Overførsel til usikre tredjelande

Der må kun må overføres persondata til usikre tredjelande, hvis der der foreligger et gyldigt overførselsgrundlag efter GDPR artikel 46-49. Overførsel til usikre tredjelande ved brug af standard contractual clauses (SCCs) kræver herudover, at der forinden overførsel er foretaget en undersøgelse af, om det pågældende modtagerlands beskyttelsesniveau i det væsentligste svarer til niveauet i henhold til EU-retten. Hvis beskyttelsesniveauet i modtagerlandet er utilstrækkeligt, skal der forinden overførsel implementeres effektive supplerende foranstaltninger, som garanterer et tilstrækkeligt niveau svarende til i henhold til EU-retten (transfer impact assessement). (GDPR artikel 45-49)

Compliancemål	Complianceniveau	Prioritet
Der sker alene overførsel af persondata til usikre tredjelande på baggrund af gyldigt overførselsgrundlag.	2	P2

Undersøgelse

Vi har undersøgt, om der er identificeret overførsel af persondata til usikre tredjelande, og om der foreligger skriftlig procedure, som sikrer, at der alene overføres persondata på baggrund af gyldigt overførselsgrundlag.

Vi har inspiceret, om skriftlig procedure er opdateret og forekommer tilstrækkelig i forhold til sikring af transfer impact assessment forinden overførsel.

Vurdering

Det vurderes, at organisationen på tidspunktet for dette tilsyn, anvender databehandlere med moderselskaber i tredjelande, herunder fx USA. Organisationen har ikke identificeret disse overførsler og har ej heller identificeret et gyldigt overførselsgrundlag.

Organisationen vurderes ikke at have en procedure, som sikrer, at der alene overføres persondata på baggrund af gyldigt overførselsgrundlag.

Anbefaling

Organisationen anbefales, at identificere hvilke behandlingsaktiviteter, som anvender databehandlere i tredjelande. Derefter anbefales det, at organisationen identificerer et gyldigt overførselsgrundlag for så vidt angår anvendelsen.

Organisationen kan eventuelt anvende EU-U.S. Data Privacy Framework (DPF), jf. EU-Kommissionens tilstrækkelighedsafgørelse, jf. GDPR artikel 46.

Organisationen anbefales desuden at etablere en procedure, som sikrer, at databehandlere i tredjelande identificeres og at data alene overføres på baggrund af et gyldigt overførselsgrundlag.

Bilag 1B: Vurderingsgrundlag og anbefalinger for sikring af databeskyttelse

B. Sikring af databeskyttelse

B1. Privacy by design og privacy by default

Privacy by design og privacy by default skal indgå i overvejelserne i forbindelse med design og implementering af nye systemer, herunder ved ændringer i eksisterende systemer. Privacy by design betyder, at alle systemer til persondatabehandling skal designes, så de tager højde for beskyttelse af persondata. Privacy by default betyder, at konfigurerbare muligheder i systemer og alle standardindstillinger skal indstilles til det minimalt nødvendige for persondatabehandlingen. (GDPR artikel 25)

Compliancemål	Complianceniveau	Prioritet
Kravene om privacy by design i nye systemer og privacy by default (standardindstillinger) efterleves.	4 ✓	n/a

Undersøgelse

Vi har undersøgt, om der er etableret skriftlige procedurer eller anden dokumentation, hvori sikring af databeskyttelse gennem design og standardindstillinger er beskrevet.

Vurdering

Organisationen har gjort et godt stykke arbejde. Compliancemålet vurderes, på det foreliggende grundlag, at være opfyldt, men der kan være mulighed for forbedring i konkrete tilfælde.

Anbefaling

Ingen.

B2. Indgåelse af databehandleraftaler

Den dataansvarlige skal indgå databehandleraftaler med leverandører (databehandlere), som den dataansvarlige har valgt til at behandle persondata på sine vegne. (GDPR artikel 4, litra 7, og artikel 28).

Compliancemål	Complianceniveau	Prioritet
Der er indgået databehandleraftaler med alle databehandlere.	2 	P2

Undersøgelse

Vi har undersøgt, om der er etableret en formaliseret proces, som sikrer, at der indgås databehandleraftaler med alle databehandlere.

Vi har inspiceret, om der foreligger et opdateret register (oversigt) over databehandlere, som giver et samlet overblik over anvendte databehandlere.

Vurdering

Det vurderes, at organisationen har arbejdet med at indgå flere databehandleraftaler med databehandlere, som behandler persondata på vegne af organisationen..

Organisationen har desuden siden sidste tilsyn udarbejdet en samlet oversigt, som illustrerer, hvilke databehandleraftaler, der er indgået og hvilke der mangler at blive indgået.

Der er fortsat ikke indgået databehandleraftaler med alle databehandlere, som behandler persondata for organisationen, da det fremgår af organisationens register over databehandlere, at der ikke er indgået databehandleraftaler med alle databehandlere.

Anbefaling

Det anbefales at der indgås databehandleraftaler med alle databehandlere, som behandler persondata for organisationen.

B3. Tilsyn af databehandlere

Den dataansvarlige skal føre kontrol med, at databehandleren overholder sine forpligtigelser som beskrevet i databehandleraftalen. Der skal føres kontrol med, at databehandleren opretholder et passende beskyttelsesniveau for de personer, som er genstand for behandling (de registrerede). Kontrol kan gennemføres ved at stille spørgsmål til databehandleren eller ved at ved at gennemgå revisorerklæringer (fx ISAE 3000 GDPR erklæring) for databehandleren. (GDPR artikel 28).

Compliancemål	Complianceniveau	Prioritet
Der føres regelmæssigt tilsyn med databehandleres opfyldelse af betingelserne i databehandleraftalen.	3	P3

Undersøgelse

Vi har undersøgt, om der er etableret en formaliseret proces, som sikrer, at der føres tilsyn af databehandlere.

Vi har inspiceret, om der foreligger en opdateret tilsynsplan, som afspejler risici for de registrerede forbundet med behandlingen.

Vurdering

Det vurderes, at organisationen har arbejdet godt med at fastlægge en opdateret tilsynsplan i overensstemmelse med Datatilsynets seks tilsynskoncepter. Denne tilsynsplan indeholder både et overblik over frekvens og valg af konkret tilsynskoncept, der afspejler risiciene forbundet med databehandlingen. På tidspunktet for tilsyn er der dog ikke blevet gennemført tilsyn med organisationens databehandlere endnu.

Anbefaling

Det anbefales at organisationen gennemfører passende tilsyn af databehandlere på baggrund af den fastlagte tilsynsplan.

B4. Risikovurdering

Risici for de personer, som er genstand for behandling (de registrerede) skal evalueres på baggrund af en metode, som sikrer identificering af sandsynlighed for, at en eller flere trusler indtræder, samt identificering af konsekvenser for registrerede, hvis der sker tab af fortrolighed, integritet og tilgængelighed for persondata (risici for de registrede). På baggrund af evaluering af risici skal det vurderes, om der skal implementeres sikkerhedsforanstaltninger for at sikre et passende beskyttelsesniveau for de registrerede (GDPR artikel 32).

Compliancemål	Complianceniveau	Prioritet
Der gennemføres risikovurdering, som identificerer risici for de registreredes rettigheder og frihedsrettigheder forbundet med behandling med henblik på at sikre et passende sikkerhedsniveau.	4 ✓	n/a

Undersøgelse

Vi har undersøgt, om der er etableret en formaliseret proces for risikovurdering, som sikrer identificering af risici fo

Vi har inspiceret dokumentation for, om risikovurdering er gennemført. Vi har inspiceret, at senest gennemførte risikovurdering forekommer at identificere risici for de registrerede rettigheder og frihedsrettigheder og vi har inspiceret, om seneste risikovurdering er forelagt til godkendelse på ledelsesniveau.

Vurdering

Organisationen har gjort et godt stykke arbejde. Compliancemålet vurderes, på det foreliggende grundlag, at være opfyldt, men der kan være mulighed for forbedring i konkrete tilfælde.

Anbefaling

Ingen.

B5. Håndtering af brud på persondatasikkerheden

Et "brud på persondatasikkerheden" er typisk en hændelse (et uheld eller ved en bevidst handling), hvor persondata kommer til uvedkommendes kendskab, hvor persondata ikke er tilgængelige eller hvor personoplysninger ikke længere er retvisende. Et sådant brud vil efter omstændighederne kunne medføre en risiko for de personer, som oplysningerne vedrører (de registrerede), og i visse tilfælde skal brud anmeldelses til Datatilsynet samt meddeles til de registrerede. (GDPR art. 33 og 34).

Compliancemål	Complianceniveau	Prioritet
Brud på persondatasikkerheden håndteres i overensstemmelse med forordningen.	4 ✓	n/a

Undersøgelse

Vi har undersøgt, om der foreligger en skriftlig procedure, som sikrer, at brud på persondatasikkerheden kan håndteres.

Vi har undersøgt, om der er etableret en proces, som sikrer, at der foretages regelmæssig gennemgang af tidligere brud for at vurdere, om særlige typer af brud kan undgås i fremtiden.

Vi har inspiceret, om der er etableret et register, som giver en systematisk oversigt over alle tidligere brud.

Vurdering

Organisationen har gjort et godt stykke arbejde. Compliancemålet vurderes på det foreliggende grundlag at være opfyldt, men der kan være mulighed for forbedring i konkrete tilfælde.

Anbefaling

Ingen.

B6. Konsekvensanalyse vedrørende databeskyttelse (DPIA)

Der skal gennemføres konsekvensanalyse vedrørende databeskyttelse (DPIA) forud for behandlinger, som sandsynligvis vil indebære en høj risiko for rettigheder og frihedsrettigheder for de personer, som der skal behandles persondata om (de registrerede). Med "høj risiko for de registreredes rettigheder og frihedsrettigheder" menes de registreredes GDPR-rettigheder, herunder retten til databeskyttelse samt retten til privatliv for de registrerede i henhold til EU's charter om grundlæggende rettigheder (GDPR artikel 35).

Compliancemål	Complianceniveau	Prioritet
Der foretages ikke højrisiko behandlinger uden, at der forinden er gennemført konsekvensanalyse vedrørende databeskyttelse.	2	P2

Undersøgelse

Vi har undersøgt, om der foreligger en formaliseret proces, som sikrer identificering af højrisiko behandlinger og gennemførelse af en DPIA forud for udførelse af højrisiko behandlinger.

Vi har inspiceret, om skriftlig procedure eller anden dokumentation forekommer tilstrækkelig til at identificere højrisiko behandlinger og gennemføre en DPIA.
Vi har inspiceret dokumentation for, om seneste gennemførte DPIA forekommer i overensstemmelse med minimumskravene i artikel 35, stk. 7.

Vurdering

Organisationen har siden sidste tilsyn etableret en skriftlig politik for konsekvensanalyse. Politikken har ikke været efterprøvet af organisationen, da det på tidspunktet for tilsynet ikke har været muligt at identificere højrisikobehandlinger igennem fortegnelsen eller risikovurderinger. Organisationen mangler fortsat at etablere en formaliseret proces, som sikrer, at organisationen udarbejder tærskelvurderinger til identificering af højrisiko behandlinger og gennemfører DPIA hvor det er påkrævet.

Anbefaling

Det anbefales fortsat, at der etableres en formaliseret proces, som sikrer, at organisationen kan identificere højrisiko behandlinger på baggrund af fortegnelsen, risikovurderinger og politikken for konsekvensanalyse. Således at organisationen kan gennemføre først tærskelvurderinger i forlængelse af risikovurderingerne og dernæst (hvis relevant) en DPIA i overensstemmelse med GDPR forud for udførelse af højrisiko behandlinger.

Bilag 1C: Vurderingsgrundlag og anbefalinger for tekniske foranstaltninger

Generelt om tekniske foranstaltninger

Tekniske foranstaltninger er tiltag, der primært er implementeret via tekniske mekanismer fx hardware, software og firmware i informationssystemer, og som bidrager til at beskytte fortrolighed, integritet og tilgængelighed af organisationens informationer, herunder persondata. Der skal implementeres passende tekniske foranstaltninger, som sikrer et passende sikkerhedsniveau for de personer, som er genstand for behandling (de registrerede). Kontrollerne, som hører under temaet tekniske foranstaltninger, er inspireret af sikkerhedsstandarden ISO27001 og ISO27002.

C1. Antivirus

I et højt digitaliseret samfund, hvor truslen fra fx cyberkriminelle er meget høj, er det vigtigt, at organisationen har forholdt sig til risikoen for cyberangreb som fx ransomware. Dette vil ofte betyde, at der skal installeres antivirus på servere, databaser og medarbejdernes computere og servere. Alt efter organisationens aktiviteter kan det være nødvendigt at overveje, om andre enheder skal beskyttes mod cybertrusler. Det kan være fx være computere, som er delt mellem flere medarbejdere. Hertil kommer, at smartphones og tablets i stadig højere grad anvendes af organisationer til kommunikation og udveksling af oplysninger på lige fod med computere, og derfor kan behovet for beskyttelse med antivirus også være relevant i denne sammenhæng.

Compliancemål	Complianceniveau		Prioritet
Der er for systemer og databaser, der anvendes til behandling af persondata, installeret antivirus, som opdateres løbende.	4	✓	n/a

Undersøgelse

Vi har undersøgt, at lokale computere er udstyret med antivirus (Heimdal), og, at servere også kører med Heimdal. Vi har inspiceret indstillingerne på Heimdal. Vipre anvendes til mailløsninger.

Vi har inspiceret settings i Heimdal, og at servere har implementeret det. Vi har inspiceret, at lokale bærbare også har implementeret Heimdal.

Vurdering

Organisationen har gjort et godt stykke arbejde. Compliancemålet vurderes, på det foreliggende grundlag, at være opfyldt, men der kan være mulighed for forbedring i konkrete tilfælde.

Anbefaling

Ingen.

C2. Firewall

En firewall er en digital barriere mellem organisationens eget netværk og andre netværk. En sådan firewall overvåger indgående og udgående netværkstrafik og blokerer for uønsket data baseret på allerede opsatte sikkerhedsregler. En firewall kan både være software- og hardwarebaseret.

Compliancemål	Complianceniveau	Prioritet
Der er etableret firewalls for at beskytte it-udstyr, systemer og databaser, der anvendes til behandling af persondata.	4 ✓	n/a

Undersøgelse

Vi har undersøgt, at lokale netværk er beskyttet af en fysisk firewall (Meraki).

Vi har inspiceret, at der er firewall på pc'er, og at der er en fysisk firewal (Meraki).

Vurdering

Organisationen har gjort et godt stykke arbejde. Compliancemålet vurderes, på det foreliggende grundlag, at være opfyldt, men der kan være mulighed for forbedring i konkrete tilfælde.

Anbefaling

Ingen.

C3. Segmentering af netværk

Ved at segmentere/adskille netværk kan organisationen begrænse skaden ved f.eks. hackerangreb eller malware. Alt efter organisationens størrelse, kompleksitet og typer af behandlingsaktiviteter kan det være nødvendigt at overveje om opdeling af netværk skal ske på baggrund af tillidsniveauer (f.eks. offentligt domæne, pc-domæne, serverdomæne), på baggrund af organisatoriske enheder (f.eks. HR, økonomi, marketing) eller en kombination af begge (f.eks. serverdomæne koblet til flere organisatoriske enheder). Med "segmentering (adskillelse) af egne netværk" menes, at organisationen har opdelt sin netværksinfrastruktur i to eller flere separate netværk typisk adskilt af en firewall.

Compliancemål	Complianceniveau	Prioritet
Egne netværk er segmenteret for at begrænse adgang til systemer og databaser, der anvendes til behandling af persondata.	4 	n/a

Undersøgelse

Vi har undersøgt, om interne netværk er segmenteret for at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af persondata.

Vi har inspiceret, at lokale wifi er opdelt i internt- og gæste-wifi.

Vurdering

Organisationen har gjort et godt stykke arbejde. Compliancemålet vurderes, på det foreliggende grundlag, at være opfyldt, men der kan være mulighed for forbedring i konkrete tilfælde.

Anbefaling

Ingen.

C4. Adgangsstyring

Alt efter organisationens størrelse og kompleksitet kan det være nødvendigt at udarbejde en procedure for at administrere brugeres (fx ansattes) systemadgange – fx deres adgang til persondata En sådan administration af brugeradgange til persondata skal være begrundet i brugernes arbejdsbetingede behov og skal forebygge, at brugerne ikke kan tilgå oplysninger, som de ikke har behov for at anvende.

Compliancemål	Complianceniveau	Prioritet
Adgang til persondata er isoleret til brugere med arbejdsbetinget behov herfor.	4 ✓	n/a

Undersøgelse

Vi har undersøgt, at der en procedure for adgange til de forskellige systemer. Vi har inspiceret processen for godkendelse af brugere (både oprettelse og sletning).

Vi har undersøgt adgange til systemer, og påset, at der er legacy-systemer, som ikke understøtter rolle opdeling, dog bliver disse løbende udfaset.

Vi har undersøgt, at de gennemgår lister over adgange løbende.

Vi har inspiceret, at der en procedure for adgange til de forskellige systemer. Vi har inspiceret processen for godkendelse af brugere (både oprettelse og sletning).

Vurdering

Organisationen har gjort et godt stykke arbejde. Compliancemålet vurderes, på det foreliggende grundlag, at være opfyldt, men der kan være mulighed for forbedring i konkrete tilfælde.

Anbefaling

ingen.

C5. Logning

Logning er et vigtigt redskab til at kortlægge, f.eks. hvordan brugere af et it-system har ageret. Logningen/registreringen af brugernes adfærd gengives i en såkaldt logoversigt eller logfil, som efterfølgende kan anvendes til bl.a. at analysere og dokumentere eventuelt misbrug af oplysninger. Logning kan i øvrigt også være et vigtigt værktøj til at opdage eventuelle hackere eller andre uvedkommendes adgang til organisationens systemer.

Compliancemål	Complianceniveau		Prioritet
Der er etableret logning og denne er beskyttet mod manipulation og uautoriseret adgang.	2		P2

Undersøgelse

Vi har undersøgt, at der er logning på servere (følger MS-standard settings i forhold til retention).

Vi har undersøgt, om de har en dedikeret logserver.

Vurdering

Det vurderes, at logfiler ikke bliver opsamlet på en logserver.

Det vurderes, at organisationen ikke har en overordnet logningsstrategi, men at de over de næste 12 måneder planlægger at implementere en løsning.

Anbefaling

Det anbefales at lave en overordnet logningsstrategi, som med fordel kan tage udgangspunkt i ISO 27001/27002 kontrollerne.

C6. Systemovervågning

Systemovervågning (monitorering) hjælper med at forebygge, opdage og korrigere potentielle sikkerhedshændelser i systemer og databaser.

Compliancemål	Complianceniveau	Prioritet
Der er for de systemer og databaser, der anvendes til behandling af persondata, etableret systemovervågning med alarmering.	4 ✓	n/a

Undersøgelse

Vi har undersøgt relevant overvågning af systemer.

Vi har inspiceret, at Heimdal overvåger patching af servere og beskyttelse mod malware.

Vurdering

Organisationen har gjort et godt stykke arbejde. Compliancemålet vurderes, på det foreliggende grundlag, at være opfyldt, men der kan være mulighed for forbedring i konkrete tilfælde.

Anbefaling

Ingen.

C7. Kryptering af harddisk og/eller filsystem

Kryptering er en sikkerhedsforanstaltning, som bl.a. beskytter oplysninger mod uvedkommende adgang. Med "kryptering af harddisk og/eller filsystem" menes en software- eller hardwarebaseret krypteringsløsning, der sikrer, at indholdet er krypteret før indtastning af brugerens password. Ved harddisk kryptering (full disk encryption) er harddiskens indhold altid krypteret, og kun dele dekrypteres og placeres i hukommelsen (RAM) ved brug. Ved kryptering af filsystemet sikres indholdet af hele/dele af filsystemet, men ikke selve operativsystemet/systemfiler, mv. Eksempler på kendte software løsninger er BitLocker(Microsoft), FileVault (Apple), LUKS (Linux) eller VeraCrypt (IDRIX).

Compliancemål	Complianceniveau		Prioritet
Der er implementeret kryptering af harddisk og/eller filsystemer på medarbejdernes computere for at beskytte persondata.	3		P3

Undersøgelse

Vi har undersøgt, om der er implementeret kryptering af harddisk og/eller filsystemer på medarbejdernes computere.

Vurdering

Det vurderes, at kryptering er slået til på storage niveau, men ikke på system-niveau.

Det er positivt, at organisationen kigger på en MDM-løsning, som også kan håndtere kryptering.

Anbefaling

Det anbefales, at organisationen vurderer, om lokale bærbare skal have bitlocker slået til.

C8. Kryptering ved overførsel via internettet

Når oplysninger sendes over åbne netværk som f.eks. internettet, har man som afsender eller modtager som udgangspunkt ingen kontrol over, hvilke maskiner (servere m.v.) de konkrete oplysninger passerer igennem undervejs, herunder hvor i verden disse maskiner er lokaliseret. For at sikre sig mod, at de overførte oplysninger tilgås af uvedkommende, kan man anvende kryptering. Med "overførsel" menes ikke kun transmission af oplysninger med e-mails, men også anden form for transmission af personoplysninger over netværk, som organisationen ikke har fuld kontrol over.

Compliancemål	Complianceniveau		Prioritet
Der anvendes effektiv kryptering ved overførsel af fortrolige og følsomme personoplysninger via internettet og med e-mail.	4	✓	n/a

Undersøgelse

Vi har undersøgt om fortrolige og følsomme personoplysninger krypteres ved overførsel via internettet fx via HTTPS eller FTPS, og/eller med e-mail.

Vi har stikprøvevis inspiceret implementering af TL på hjemmesider.

Vurdering

Organisationen har gjort et godt stykke arbejde. Compliancemålet vurderes, på det foreliggende grundlag, at være opfyldt, men der kan være mulighed for forbedring i konkrete tilfælde.

Anbefaling

Ingen.

C9. Sårbarhedsscanninger og penetrationstest

Sårbarhedsscannere kan tjekke systemer for at verificere, at operativsystemet er opdateret, har opdateret antivirussoftware og har en aktiveret firewall, herunder verifiere at systemer ikke kører visse tjenester og protokoller, som kan blive udnyttet af trusler. Penetrationstest går videre end sårbarhedsscanninger og forsøger at udnytte de opdagede sårbarheder for at vise, i hvilket omfang det er muligt at opnå uatoriseret adgang til netværk, systemer, databaser, servere og persondata.

Compliancemål	Compliancenіveau	Prioritet
De etablerede tekniske foranstaltninger testes løbende ved sårbarhedsscanninger og/eller penetrationstests.	4 ✓	n/a

Undersøgelse

Vi har undersøgt, om de etablerede tekniske foranstaltninger løbende testes ved sårbarhedsscanninger og/eller penetrationstests.

Vi har inspiceret IT-analysen, og forespurgt til relevante findings.

Vurdering

Organisationen har gjort et godt stykke arbejde. Compliancemålet vurderes, på det foreliggende grundlag, at være opfyldt, men der kan være mulighed for forbedring i konkrete tilfælde.

Anbefaling

Ingen

C10. Opdateringer og patches

Leverandører udgiver regelmæssigt patches, rettelser og opdateringer. Grundlæggende hærdningspraksis sikrer, at systemerne har alle relevante patches installeret, inklusive patches til operativsystemer og applikationer, herunder sikkerhedspatches, som har til formål at lukke sikkerhedshuller i programmer.

Compliancemål	Complianceniveau	Prioritet
Der er etableret en proces for regelmæssigt at opdatere og patche i programmer, styresystemer og andre softwareløsninger.	4 	n/a

Undersøgelse

Vi har undersøgt om der er etableret en proces for regelmæssigt at opdatere og patche i programmer, styresystemer og andre softwareløsninger.

Vi har inspiceret, at systemer bliver løbende opdateret, og det bliver dokumenteret i seperat excel-ark.

Vurdering

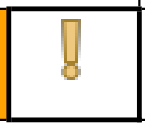
Organisationen har gjort et godt stykke arbejde. Compliancemålet vurderes, på det foreliggende grundlag, at være opfyldt, men der kan være mulighed for forbedring i konkrete tilfælde.

Anbefaling

Ingen.

C11. To-faktor autentifikation

Med "to-faktor-autentifikation" menes en login-proces, som indebærer to godkendelseselementer. Man taler typisk om, at et sådant godkendelseselement er: ”Noget man ved” (brugernavn i kombination en adgangskode), ”Noget man har” (et nøglekort eller en pc, som – via et på forhånd installeret certifikat – kan genkendes af den it-løsning, som forsøges tilgået) og ”Noget man er” (et fingeraftryk eller en iris-skanning). Det er kombinationen af to af disse elementer, der udgør de to faktorer.

Compliancemål	Complianceniveau	Prioritet
Der implementeret to-faktor-autentifikation ved adgang til systemer og databaser, hvori der sker behandling af persondata, der medfører høj risiko for de registrerede.	2 	P2

Undersøgelse

Vi har undersøgt, om adgang til systemer og databaser, hvori der sker behandling af persondata, som minimum sker ved anvendelse af to-faktor autentifikation.

Vi har stikprøvevis inspiceret adgange til systemer.

Vurdering

Ved adgang til Heimdal, anvendes der to-faktor. For at komme på VPN kræves et privat-certifikat. Der anvendes ikke traditionel to-faktor, da mange systemer ikke kan understøtte det. Organisationen er i gang med at vurdere, hvor to-faktor kan implementeres.

Anbefaling

Det anbefales, at organisationen vurderer, hvordan den kan sikre, at der anvendes to-faktor på relevante systemer.

C12. Backup

Backup er en kopi af organisationens data således, at organisationen til enhver tid har en (forholdsvis opdateret) kopi af sine data til rådighed – de aktuelt anvendte data, der opdateres løbende, samt backup-kopien, der er et historisk øjebliksbillede. Jo længere tid, der går mellem, at organisationen opretter og gemmer en backup-kopi af sine data, desto større forskel vil der normalt være mellem de aktuelt anvendte data og den seneste backup-kopi. Backup-kopien bør opbevares adskilt fra de aktuelt anvendte data og skal sikre, at organisationen kan genetablere it-driften, hvis de aktuelt anvendte data går tabt eller bliver beskadiget. Dette kunne f.eks. være relevant, hvis hackere har udnyttet en sårbarhed hos organisationen og har krypteret oplysninger.

Compliancemål	Complianceniveau		Prioritet
Der foretages backup af data og persondata med regelmæssige mellemrum.	4	✓	n/a

Undersøgelse

Vi har undersøgt om der foretages backup af data og persondata med regelmæssige mellemrum.

Vi har inspiceret backuprutine for de enkelte servere.

Vurdering

Organisationen har gjort et godt stykke arbejde. Compliancemålet vurderes, på det foreliggende grundlag, at være opfyldt, men der kan være mulighed for forbedring i konkrete tilfælde.

Anbefaling

Ingen.

Bilag 1D: Vurderingsgrundlag og anbefalinger for organisatoriske foranstaltninger (governance)

Generelt om organisatoriske foranstaltninger (governance)

Organisatoriske foranstaltninger fokuserer på styringen af beskyttelse af organisationens informationer, herunder persondata. Organisatoriske foranstaltninger kan fx omfatte administrative handlinger, politikker, procedurer, retningslinjer mv. til at styre, implementere, vedligeholde og forankre håndtering og beskyttelse af organisationens informationer, herunder persondata. Kontrollerne under temaet "organisatoriske foranstaltninger" er inspireret af kontroller fra sikkerhedsstandarden ISO27001 og ISO27002.

D1. Politik for informationssikkerhed

En politik for informationssikkerhed fastsætter, på et overordnet niveau, principper for hvad organisationen, herunder medarbejderne, skal gøre i forhold til beskyttelsen af bl.a. it-systemer, computere, mobile enheder og informationer, herunder persondata. En politik for informationssikkerhed ved behandling af persondata bør afspejle, hvordan persondata skal håndteres og beskyttes i organisationen under hensyntagen til risici for de personer, som der behandles persondata om (de registrerede).

Compliancemål	Complianceniveau	Prioritet
Der er en opdateret politik for informationssikkerhed ved behandling af persondata, som er godkendt på ledelsesniveau.	4 ✓	n/a

Undersøgelse

Vi har undersøgt, om der er en opdateret politik for informationssikkerhed ved behandling af persondata, som er godkendt på ledelsesniveau.
Vi har undersøgt, om politikken kommunikeres til medarbejderne i organisationen.

Vi har inspiceret, om politik for informationssikkerhed ved behandling af persondata forekommer tilstrækkelig for opretholdelse af databeskyttelsessikkerhed i organisationen, herunder om politikken kommunikeres til medarbejderne.

Vurdering

Organisationen har gjort et godt stykke arbejde. Compliancemålet vurderes på det foreliggende grundlag at være opfyldt, men der kan være mulighed for forbedring i konkrete tilfælde.

Anbefaling

Ingen.

D2. Roller og ansvar

Der skal være en fordeling af ansvar med hensyn til, hvem der skal varetage de enkelte GDPR-opgaver for sikring af databeskyttelse (fx risikovurderinger, tilsyn af databehandlere og håndtering af brud på persondatasikkerheden). På området for informationssikkerhed vil der normalt være udpeget en person, som er ansvarlig for informationssikkerhed (læs: beskyttelse af organisationens informationer) i organisationen fx it-chef, digitaliseringschef, CISO eller CTO. Alt efter organisationens størrelse og kompleksitet vil det styrke arbejdet med informationssikkerheden, hvis der er en klar ansvarsfordeling i forhold til, hvem der skal varetage de enkelte sikkerhedsopgaver.

Compliancemål	Complianceniveau		Prioritet
Der foreligger beskrevet rolle- og ansvarsfordeling med hensyn til varetagelse af GDPR- og informationssikkerhedsopgaver i organisationen.	4	✓	n/a

Undersøgelse

Vi har undersøgt, om der er foreligger en beskrevet rolle- og ansvarsfordeling med hensyn til varetagelse af GDPR- og informationssikkerhedsopgaver i organisationen.

Vi har inspiceret, om en rolle- og ansvarsfordeling for organisationens GDPR og informationssikkerheds opgaver forekommer fyldestgørende.

Vurdering

Organisationen har gjort et godt stykke arbejde. Compliancemålet vurderes på det foreliggende grundlag at være opfyldt, men der kan være mulighed for forbedring i konkrete tilfælde.

Anbefaling

Ingen.

D3. Ledelsesforankring

Ledelsen sætter retningen for arbejdet med informationssikkerhed og databeskyttelse i organisationen. Implementering, vedligeholdelse og forankring af informationssikkerhed, herunder databeskyttelse, afhænger af ledelsens og topledelsens involvering og engagement.

Compliancemål	Complianceniveau	Prioritet
Arbejdet med informationssikkerhed og databeskyttelse efter GDPR er forankret på ledelsesniveau.	4 ✓	n/a

Undersøgelse

Vi har undersøgt, om der er etableret et sikkerhedsudvalg eller anden "styregruppe" med deltagelse på ledelsesniveau, som regelmæssigt håndterer spørgsmål om informationssikkerhed og databeskyttelse.

Vurdering

Organisationen har gjort et godt stykke arbejde. Compliancemålet vurderes på det foreliggende grundlag at være opfyldt, men der kan være mulighed for forbedring i konkrete tilfælde.

Anbefaling

Ingen.

D4. Årshjul

Alt efter organisationens størrelse og kompleksitet kan det være nødvendigt systematisk at kontrollere, at væsentlige politikker og retningslinjer vedrørende informationssikkerhed og databeskyttelse er ajourførte og opdaterede med faste intervaller. I et årshjul kan organisationen på overskuelig vis samle information om de aktiviteter, der skal gennemføres, og fastlægge datoer og ansvar for, at aktiviteterne bliver gennemført.

Compliancemål	Complianceniveau	Prioritet
Der er etableret et årshjul, som understøtter, at alle væsentlige politikker, retningslinjer mv. vedrørende informationsikkerhed og databeskyttelse følges.	3	P3

Undersøgelse

Vi har undersøgt, om der er etableret et årshjul, som understøtter at alle væsentlige politikker, retningslinjer mv. vedrørende informationssikkerhed og databeskyttelse følges.

Vurdering

Det vurderes, at organisationen har et årshjul, som understøtter opgaver vedrørende informationssikkerhed. Organisationen har dog fortsat ikke etableret et årshjul, som understøtter opgaver vedrørende databeskyttelse (fx løbende risikovurderinger og tilsyn med databehandlere)

Anbefaling

Det anbefales, at organisationen får etableret et årshjul, som understøtter opgaver vedrørende databeskyttelse.

D5. Uddannelse/Awareness

Der skal gennemføres uddannelse af medarbejdere med henblik på at sikre ønsket adfærd og opmærksomhed omkring beskyttelse af organisationens infomationer, herunder håndtering og beskyttelse af persondata. Udddannelse kan være interne eller eksterne kurser om sikkerhed på arbejdspladsen og om behandling af persondata, som er relevante for medarbejdernes løsning af arbejdsopgaver og deres generelle adfærd. Sådan en uddannelse, ofte kaldt awareness-træning, kan også bestå af interne oplæg, møder og workshops, hvor forsvarlig adfærd og relevante scenarier drøftes. Det kan typisk være relevant at gennemføre awareness-træning for nye medarbejdere som en del af deres introduktion (onboarding). Alt efter organisationens størrelse og kompleksitet - og ved større organisatoriske ændringer - kan det være nødvendigt at gennemføre regelmæssig awareness-træning, så medarbejderne kan holde sig ajour med organisationens politikker og retningslinjer i det omfang, det er relevant for deres jobfunktion.

Compliancemål	Complianceniveau	Prioritet
Medarbejderne uddannes løbende i it-sikkerhed og databeskyttelse.	4 ✓	n/a

Undersøgelse

Vi har undersøgt, om medarbejdere løbende uddannes i it-sikkerhed og databeskyttelse. Vi har undersøgt, om der følges op på, om medarbejderne gennemfører uddannelse. Vi har undersøgt, om eventuel politik for informationssikkerhed indgår i uddannelsen af medarbejderne.

Vurdering

Organisationen har gjort et godt stykke arbejde. Compliancemålet vurderes på det foreliggende grundlag at være opfyldt, men der kan være mulighed for forbedring i konkrete tilfælde.

Anbefaling

Ingen.

D6. Business Recovery Plan/beredskab

Det er relevant, i en beredsskabsplan, at tage stilling til, hvordan driften af kritiske forretningsopgaver opretholdes, hvis organisationen ikke længere har adgang til vigtige it-systemer. Kritiske forretningsopgaver er typisk arbejdsrelaterede opgaver, der er vigtige at udføre for at undgå eller begrænse (større) negative konsekvenser for organisationen og de registrerede.

Compliancemål	Complianceniveau		Prioritet
Der er etableret en beredskabsplan for opretholdelse af kritiske forretningsopgaver.	4	✓	n/a

Undersøgelse

Vi har undersøgt om der er etableret en beredskabsplan.

Vi har undersøgt om der foretages regelmæssige test af beredskabsplanen.

Vi har inspiceret, at beredskabsplan forekommer tilstrækkelig for opretholdelse af kritiske forretningsopgaver.

Vurdering

Organisationen har gjort et godt stykke arbejde. Compliancemålet vurderes, på det foreliggende grundlag, at være opfyldt, men der kan være mulighed for forbedring i konkrete tilfælde.

Anbefaling

Ingen.

D7. Disaster Recovery Plan/genetablering af it-systemer og it-drift

Det er også relevant at tage stilling til, hvordan organisationen får genetableret it-systemer og den normale it-drift i tilfælde af nedbrud fx i tilfælde af hackerangreb, brand, oversvømmelser, tyveri og strømsvigt. Dette indebærer først og fremmest en stillingtagen til ansvars- og rollefordelingen i organisationen, hvis uheldet er ude. Alt efter organisationens karakter kan det også indebære en forudgående kortlægning af bl.a. centrale opgaver og processer, prioritering af ressourcer og systemer samt fastlæggelse af kommunikationskanaler.

Compliancemål	Complianceniveau	Prioritet
Der er etableret en plan for genetablering af it-systemer og it-drift.	4 ✓	n/a

Undersøgelse

Vi har undersøgt, om der er etableret en plan for genetablering af it-systemer og it-drift i tilfælde af nedbrud.

Vurdering

Organisationen har gjort et godt stykke arbejde. Compliancemålet vurderes på det foreliggende grundlag at være opfyldt, men der kan være mulighed for forbedring i konkrete tilfælde.

Anbefaling

Ingen.

D8. Fysisk sikkerhed

Det er relevant at sikre, at der ikke kan opnås adgang for uautoriserede personer til lokaliterer, hvori der opbevares og behandles persondata (fx arkiver, serverrum og kontorer). Fysisk adgangssikkerhed kan bl.a. opnås ved at aflåse lokaler, herunder at afskærme vinduer, hvis sådanne kan udnyttes af uatoriserede personer til at få kiggeadgang til persondata.

Compliancemål	Complianceniveau	Prioritet
Der er etableret fysisk adgangssikkerhed for lokaliteter, hvori der opbevares og behandles persondata.	4 ✓	n/a

Undersøgelse

Vi har undersøgt, om der er etableret fysisk adgangssikkerhed til serverrummet hos organisationen, således at kun autoriserede personer kan opnå fysisk adgang til lokaliteter, hvori der opbevares og behandles persondata.

Vurdering

Organisationen har gjort et godt stykke arbejde. Compliancemålet vurderes på det foreliggende grundlag at være opfyldt, men der kan være mulighed for forbedring i konkrete tilfælde.

Anbefaling

Ingen.

Bilag 2: Årets handlinger

Udførte handlinger gennem året	
Afsluttet	NOP og konsekvensanalyse/risikovurdering
Afsluttet	Rapport og præsentation for ledelse
Afsluttet	NIS2 direktivet og fremtidige tilsyn?
Afsluttet	Videregivelse til arbejdsmarkedets parter
Afsluttet	Spørgsmål vedr. videregivelse mellem 2 DA
Afsluttet	DBA med Miralix
Afsluttet	Google Analytics
Afsluttet	TITsam kontrakt
Afsluttet	Udfærdigelse af dokumentation for NT
Afsluttet	DPO audit D6
Afsluttet	Indhent pris på Wired til NT
Afsluttet	Spørgsmål vedr. løsning til vagtsamling
Afsluttet	Henvendelse fra NT angående spørgsmål fra marketingafdeling vedr. anvendelse af rejsekortkunders telefonnumre
Afsluttet	TITsam kontrakt
Afsluttet	Udfærdigelse af dokumentation for NT
Afsluttet	DPO audit D6
Afsluttet	Udlevering af persondata mellem NT og NJ medarbejder
Afsluttet	Rapportens anbefalinger
Afsluttet	Dato for næste tilsyn i marts
Afsluttet	Spørgmål vedrørende "tilgængelighed" både på web og i forhold til digital post

Data trukket fra Monday board "Nordjyllands Trafikselskab DPO Statusmøde" d. 23-10-2023.

9. februar 2024

5. Meddelelser

Der vil på mødet blive orienteret om:

- NTtrivsel 2023 (bilag 5A)
- Økonomiske nøgletal for trafikselskaberne
- Input til dialogmøde med Ekspertudvalget den 24. januar (bilag 5B)
- Status for flextrafik i Nordjylland

Bilag
Bilag 5A, NTtrivsel 2023, overordnet resultat
Bilag 5B, Ekspertudvalg, dialogmøde med interessenter i den kollektive transport

NTtrivsel 2023 | overordnet resultat

vi rejser sammen

Samlet score og svarprocent

Samlet score

3.0 / 4

-0.1 Industri benchmark

-0.1 Ændring siden sidste undersøgelse

Høj svarprocent

96%

93 ud af 97 medarbejdere har svaret

93 Besvaret

4 Ikke besvaret

Resultater for kategorien:

Information & Retningslinjer

3.7 / 4 -0.3 Ændring siden sidste undersøgelse

SPØRGSMÅL	SCORE	CHANGE	
1.INSTRUKTION OG VEJLEDNING Har du fået den nødvendige instruktion og vejledning til at udføre dit arbejde?	3.7	-0.3	8% 0% 0% 0% 90% 2% Nej

Resultater for kategorien:

Indeklima

2.3 / 4

0.0 Ændring siden sidste undersøgelse

SPØRGSMÅL	SCORE	CHANGE	
4.TEMPERATUR & TRÆK Er du tilfreds med indeklimaet på din arbejdsplads (varmt/koldt, træk mv.)?	1.7	-0.3	14% 40% 19% 19% 8% 0%
5.STØJ OG FORSTYRRELSER Oplever du, at støjen i løbet af din arbejdsdag er så høj, at det forstyrrer din koncentration og løsning af dine opgaver?	2.5	+0.2	3% 17% 20% 42% 17% 0%
6.Støj og Forstyrrelser Har du selv mulighed for at påvirke støjniveauet (f.eks. ved at booke et "stillerum" eller lign.), når du ikke vil forstyrres?	2.8	+0.1	3% 10% 20% 34% 32% 0%

Meget utilfreds

Altid

I meget lav grad

Resultater for kategorien:

Sikkerhedskultur

3.7 / 4 -0.3 Ændring siden sidste undersøgelse

SPØRGSMÅL	SCORE	CHANGE	
7.FALD & SNUBLEN Er der steder på virksomheden, der udgør en fare for din sikkerhed? (Hvis ja, så giv straks besked om hvor til en af NT's arbejdsmiljørepræsentanter.)	3.7	-0.3	6% Ja 0% 0% 0% 94% 0%

Resultater for kategorien:

Arbejdets indhold og udførelse

3.1 / 4 -0.1 Ændring siden sidste undersøgelse

SPØRGSMÅL	SCORE	CHANGE	
8.ROLLEKLARHED Ved du, hvad der forventes af dig i dit arbejde?	3.2	-0.1	0% 4% 6% 54% 34% 1%
9.MODSTRIDENDE KRAV Hjælper din leder dig med at prioritere dine arbejdsopgaver, når det er nødvendigt?	2.9	-0.1	I meget lav grad 0% 9% 23% 38% 31% 0%
10.INTERESSANTE ARBEJDSOPGAVER Synes du, at dine arbejdsopgaver er interessante og inspirerende?	3.1	-0.1	Aldrig 1% 1% 17% 51% 30% 0%

I meget lav grad

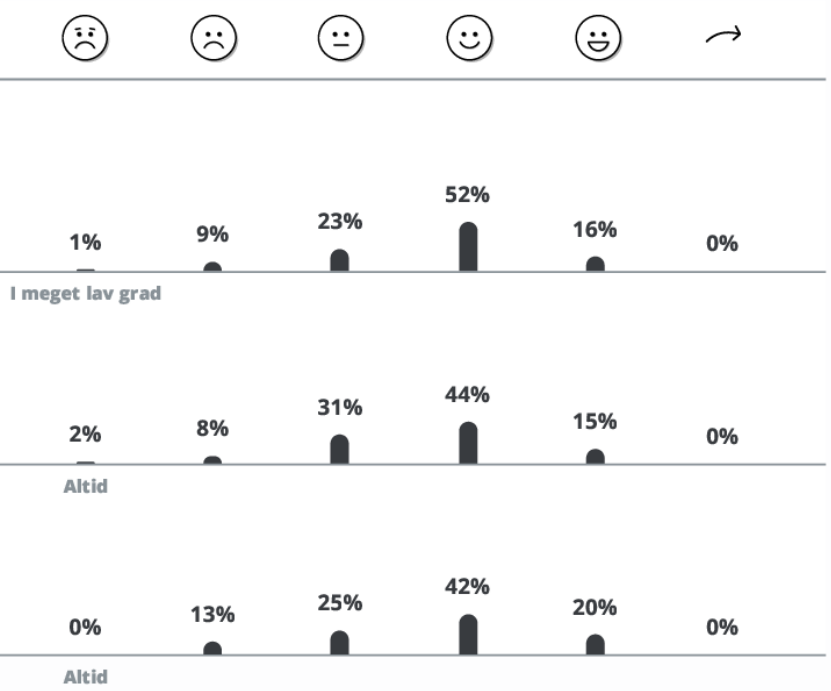
Resultater for kategorien:

Arbejdstid og -mængde

2.7 / 4

0.0 Ændring siden sidste undersøgelse

SPØRGSMÅL	SCORE	CHANGE
11.ARBEJDSMÆNGDE Trives du med din arbejdsmængde?	2.7	-0.1
12.ARBEJDSMÆNGDE Hvor ofte har du tidsfrister, der er svære at overholde?	2.6	+0.1
13.BALANCE MELLEM ARBEJDS- OG PRIVATLIV Oplever du, at dit arbejde tager så meget af din energi, at det går ud over privatlivet?	2.7	+0.0



Resultater for kategorien:

Støtte

3.0 / 4

0.0 Ændring siden sidste undersøgelse

SPØRGSMÅL	SCORE	CHANGE	
14.STØTTE FRA KOLLEGER Får du hjælp af dine kolleger, hvis du har brug for hjælp eller for meget at lave?	3.1	+0.0	0% 8% 19% 32% 41% 0%
15.KOLEGIALE RELATIONER OG STØTTE Er der en følelse af sammenhold og samhørighed blandt dig og dine kolleger?	3.1	-0.1	I meget lav grad 3% 3% 18% 33% 41% 1%
16.Kollegiale relationer og støtte Er du og dine kolleger gode til at arbejde sammen på tværs af afdelinger?	2.7	-0.1	I meget lav grad 2% 6% 28% 48% 15% 0%
17.Kollegiale relationer og støtte Er du fleksibel ift. at tage ekstraarbejde, når der er behov for det?	3.4	+0.0	I meget lav grad 0% 0% 9% 45% 47% 0%

Aldrig

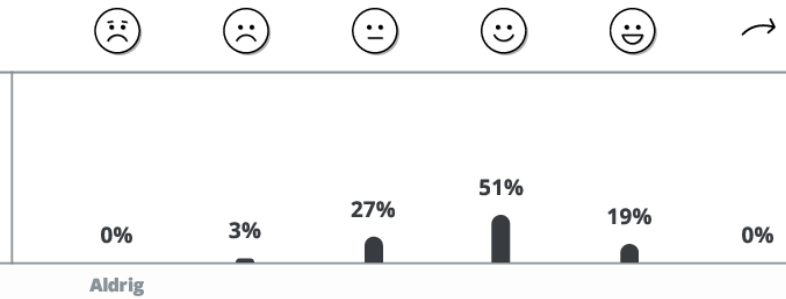
Resultater for kategorien:

Støtte

3.0 / 4

0.0 Ændring siden sidste undersøgelse

SPØRGSMÅL	SCORE	CHANGE
18.Kollegiale relationer og støtte Oplever du, at kollegerne er fleksible ift. at tage ekstraarbejde, når der er behov for det?	2.9	+0.1



Resultater for kategorien:

Nærmeste ledelse

3.0 / 4

0.0 Ændring siden sidste undersøgelse

SPØRGSMÅL	SCORE	CHANGE	1	2	3	4	5	→
19.STØTTE FRA NÆRMESTE LEDER Tager din nærmeste leder hensyn til dine behov og synspunkter, når han eller hun træffer beslutninger?	2.9	-0.1	1%	4%	22%	45%	28%	0%
20.STØTTE FRA NÆRMESTE LEDER Får du den hjælp og støtte, du har brug for fra din nærmeste leder?	3.1	+0.0	0%	5%	23%	31%	41%	0%
21.SAMARBEJDE MED NÆRMESTE LEDER Involverer din nærmeste leder dig i tilrettelæggelsen og planlægningen af dit arbejde?	2.9	+0.0	0%	3%	25%	46%	26%	0%
22.ANERKENDELSE FRA NÆRMESTE LEDER I hvor høj grad bliver dit arbejde anerkendt og påskønnet af din nærmeste leder?	3.1	+0.1	1%	3%	19%	37%	40%	0%

1: I meget lav grad
2:
3:
4:
5: Aldrig
→:

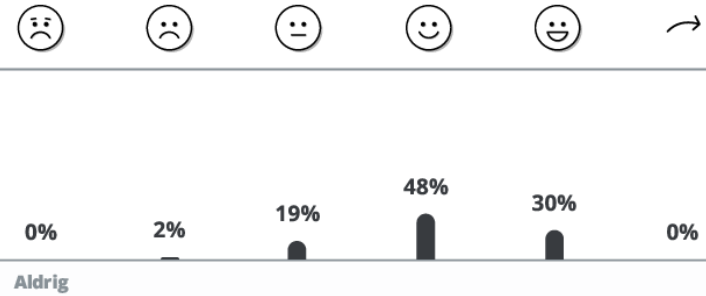
Resultater for kategorien:

Nærmeste ledelse

3.0 / 4

0.0 Ændring siden sidste undersøgelse

SPØRGSMÅL	SCORE	CHANGE
23.TILLID TIL NÆRMESTE LEDER Har du tillid til de beslutninger, som din nærmeste leder træffer?	3.1	+0.0



Resultater for kategorien:

Krænkende handlinger

3.8 / 4 Ingen data **Ændring siden sidste undersøgelse**

SPØRGSMÅL	SCORE	CHANGE						
24.TRUSLER OM VOLD Har du inden for de sidste 2 år været udsat for trusler i forbindelse med dit arbejde? Med trusler menes mundtlige eller skriftlige trusler eller truende adfærd.	3.2	-0.1	20%	0%	0%	0%	80%	0%
25.FYSISK VOLD Har du inden for de sidste 2 år været udsat for fysisk vold i forbindelse med dit arbejde?	4.0	+0.0	Ja 0%	0%	0%	0%	100%	0%
26.MOBNING Har du været udsat for mobning på dit arbejde inden for de sidste 2 år? Mobning finder sted, når en person gentagne gange og over længere tid bliver udsat for ubehagelige eller negative handlinger på sit arbejde. For at kunne sige at noget er mobning, må den, der bliver mobbet, føle, at det er svært at forsvare sig.	3.9	+0.0	Ja 3%	0%	0%	0%	97%	0%
27.SEKSUEL CHIKANE Har du inden for de sidste 2 år været udsat for seksuel chikane på din arbejdsplads?	4.0	+0.0	Ja 1%	0%	0%	0%	99%	0%

Resultater for kategorien:

Stress & burnout

2.7 / 4

0.0 Ændring siden sidste undersøgelse

SPØRGSMÅL	SCORE	CHANGE	
28.STRESS PGA. ARBEJDET I hvilken grad har du oplevet stresssymptomer i den seneste tid? Fx manglende overblik, dårlig søvn, ekstra mange bekymringer m.m.	2.7	Ingen data	3% 15% 19% 35% 27% 0% I meget høj grad

Resultater for kategorien:

Engagement

3.0 / 4 -0.2 Ændring siden sidste undersøgelse

SPØRGSMÅL	SCORE	CHANGE	
29.JOBTILFREDSHED Hvor tilfreds er du med dit job alt i alt?	3.2	-0.1	0% 2% 8% 63% 27% 0%
30.JOBTILFREDSHED Oplever du, at NT er et godt sted at arbejde	3.2	-0.2	Meget utilfreds 0% 1% 15% 52% 32% 0%
31.ENGAGEMENT OG GLÆDE Giver dit arbejde dig selvtillid og arbejdsglæde?	2.9	-0.2	I meget lav grad 0% 3% 18% 58% 19% 1%
32.ENGAGEMENT OG GLÆDE Er du stolt over det resultat, vi opnår på arbejdspladsen?	2.9	-0.2	I meget lav grad 0% 6% 20% 54% 19% 0% I meget lav grad

Resultater for kategorien:

Engagement

3.0 / 4

-0.2 Ændring siden sidste undersøgelse

SPØRGSMÅL	SCORE	CHANGE	
33.ENGAGEMENT OG GLÆDE Vil du anbefale NT som arbejdsplads til andre?	3.1	-0.1	0% 5% 14% 47% 33% 0%

I meget lav grad

Resultater for kategorien:

Sygefravær

3.9 / 4

0.0 Ændring siden sidste undersøgelse

SPØRGSMÅL	SCORE	CHANGE	
34.SYGEFRAVÆR Et godt arbejdsmiljø kan bidrage til et lavt sygefravær, ligesom det modsatte kan være tilfældet. Er der forhold i arbejdsmiljøet, der øger dit sygefravær?	3.9	+0.0	3% 0% 0% 0% 97% 0% Ja

vi rejser sammen

Transportministeriet
Frederiksholms kanal 27 F
1220 København K

mobsek@trm.dk

15. januar 2024

Ekspertudvalg om kollektiv mobilitet i hele Danmark | dialogmøde med interessenter i den kollektive transport

Kære Helga Theil Thomsen, formand for ekspertudvalget,

Først og fremmest en stor tak for invitationen til dialogmøde med Ekspertudvalg om kollektiv mobilitet i hele Danmark. Undertegnede deltager på vegne af Nordjyllands Trafikselskab (NT) og ser frem til en spændende og iderig diskussion med et bredt udsnit af interessenter fra transportsektoren i Danmark.

Vi forstår dialogmødet sådan, at det vedrører udvalgets arbejde med en kortlægning af borgernes transportbehov og udvikling af et katalog over nye kollektive mobilitetstilbud til forskellige geografier. Som forberedelse til dialogmødet har I bedt om vores indspark til en række konkrete spørgsmål, som vi kort vil besvare i nedenstående, med udgangspunkt i vores eget perspektiv.

Trafikselskaberne – brancheforeningen for de seks regionale trafikselskaber i Danmark – har tidligere fremsendt pjecen "Styrk mobiliteten i landområderne – trafikselskabernes bud på løsninger" til Ekspertudvalget. I forhold til dialogmødet vil vi derfor også her slå et slag for indholdet i denne pjece, som vi håber naturligt indgår i udvalgets kortlægning af nuværende og fremtidige mobilitetsløsninger og de barrierer, der eksisterer for deres (fortsatte) implementering.

(1) Hvordan kan den kollektive mobilitet styrkes?

Helt overordnet har vi en god og velfungerende kollektiv trafik i Danmark. På landsdelstrafikken er det statens jernbanetrafik, suppleret af fuldt kommercielle ekspresbusser, der udfylder kundernes behov for mobilitet. Tilsvarende er det trafikselskabernes kerneprodukter – lokaltog, busser og flextrafik – der regionalt og lokalt udfylder kundernes behov for mobilitet.

I Nordjylland har vi igennem de seneste mange år bestræbt os på løbende at udvikle vores løsninger, så de til stadighed har kundernes skiftende mobilitetsbehov for øje. Vores seneste

Nordjyllands Trafikselskab
John F. Kennedys Plads 1T, 3. Sal
9000 Aalborg

Tlf.: +45 9934 1111
Fax: +45 9934 1101
info@NTmail.dk

tiltag i det øjemed er vores samlende tiltag i forhold til den kollektive trafik i Nordjylland kaldet ”Fremtidens kollektive trafik”. Udgangspunktet i ’Fremtidens kollektive trafik’ er at sikre den bedst mulige mobilitet og service for pengene, så vi kan tiltrække endnu flere kunder indenfor samme økonomi som i dag. Ambitionen er at være der, hvor kunderne er, og gøre kollektiv trafik så attraktiv som muligt. Det gør vi ved at styrke og forbedre vores kerneprodukter:

- **Forenklede fleksible produkter** | for NT er de fleksible produkter en fuldt integreret del af den kollektive trafik. Produkter som ”Plustur” og ”Flextur” er igennem de seneste år blevet optimeret og forenklet, senest bl.a. med en forenkling af takster og rejseregler i Nordjylland. Vi skal dog endnu længere med forenklingen og bl.a. sikre den fulde integration til de kommende digitale billetteringsløsninger fra Rejsekort & Rejseplan.

- **Knudepunkter, der indbyder til mere end blot at vente** | vi glemmer ofte, at stoppestedet eller stationen, er indgangen til den kollektive trafik. Derfor skal disse essentielle knudepunkter naturligvis have en standard der gør, at nye og potentielle kunder ønsker at træde indenfor i butikken. Derfor skal de have et højt, ensartet serviceniveau med rene og indbydende omgivelser, et ensartet udtryk og god og relevant information. For at sikre dette, har NT overtaget budgetansvaret for >200 knudepunkter i det nordjyske hovednet, som en del af ”Fremtidens kollektive trafik”.

- **Flere afgange i vores nordjyske ”expresbus” koncept** | ”få stop - hurtigt frem”. Det er den helt store fordel ved ekspresbusserne, som skaber sammenhæng i de store transportkorridorer mellem vores større byer i Nordjylland. Vi har haft stor succes med at tiltrække kunder til vores lokaltog, og ser et potentiale i at indsætte flere ”tog på gummihjul”.

Hvis den kollektive mobilitet i Nordjylland skal styrkes inden for rammerne af den nuværende økonomi, mener vi, at ovenstående nytænkning af det samlede system er vejen frem. Investeringen i de store transportkorridorer via flere ekspresbusser sker på bekostning af primært regionale busser med et mindre passagergrundlag. Det er naturligvis en hårfin balance, og vi skal være meget opmærksomme på de skævvridninger, det kan skabe i mobilitetsudbuddet mellem by og land i vores region. I det tilfælde, at vi i Danmark ikke ønsker at investere yderligere i kollektive mobilitetsløsninger, er det dog en præmis, vi er nødt til at arbejde med.

I Nordjylland arbejder vi meget stringent med eksekveringen af vores egen strategi- og mobilitetsplan, som er bundet tæt op på tilsvarende ved vores kommunale og regionale ejere. Vi ser det som en styrke, at vi lokalt arbejder mod forankrede fælles strategier og mål for mobiliteten i Nordjylland, og kunne godt efterspørge tilsvarende på et nationalt plan i Danmark.

Nordjyllands Trafikselskab
John F. Kennedys Plads 1T, 3. Sal
9000 Aalborg

Tlf.: +45 9934 1111
Fax: +45 9934 1101
info@NTmail.dk

Bestyrelse og repræsentantskab i NT besøgte sidste efterår provinserne Groningen, Drenthe og Friesland i Holland. Et land, der i mange henseender minder om vores eget – også i forhold til den kollektive trafik og generelle mobilitet. Her har man med fordel udarbejdet en samlende national mobilitetsplan, der bl.a. udstikker retning og mål for området. Ligeledes har man hos vores svenske naboer, igennem mere end 10 år arbejdet mod en ambition omkring en fordobling af antallet af rejsende i den kollektive trafik.

Noget tilsvarende kunne tænkes at bidrage til en styrket og endnu mere sammenhængende kollektiv mobilitet i Danmark, forudsat den nødvendige eksekveringskraft og investeringsvilje bag planerne.

(2) Hvilke mobilitetsløsninger (eksisterende og nye/ukendte) ser din organisation som en del af den fremtidige kollektive mobilitet?

De sidste 10-15 år har vi set en bred palette af nye mobilitetsløsninger lanceret. Mange af løsningerne, f.eks. delecykler, samkørsel og delebiler, er løsninger som har eksisteret i mange år, men som har gennemgået en fornyelse med udbredelsen af smartphones. De moderne løsninger er ofte fuldt kommercielle og deraf primært udrullede i større byer, hvor den fuldt kommercielle forretningsmodel er økonomisk bæredygtig.

I Nordjylland så vi tidligt muligheder i de moderne mobilitetsløsninger, og lancerede bl.a. tilbage i 2018 den multimodale rejseplanlægger ”MinRejseplan”, som integrerede flere af disse nye løsninger. Fælles for mange af de nye mobilitetsløsninger er nemlig, at de ofte er ”stand-alone” løsninger uden større sammenhæng eller integration – f.eks. i forhold til rejsesøgning og billettering – til konkurrerende løsninger eller klassisk kollektiv trafik. Derudover er de fleste nye mobilitetsløsninger – helt naturligt – begrænsede i deres geografiske udrulning, grundet de fuldt kommercielle forretningsmodeller.

Hvis disse nye mobilitetsløsninger skal udbredes yderligere og blive en naturlig del af det sammenhængende mobilitetsudbud, kræver det nytænkning af de overordnede rammebetingelser for den kollektive mobilitet i Danmark. Det kunne f.eks. ske ved, at de regionale trafikselskaber fik større mulighed for at subsidiere eller udbyde disse lokalt eller fik mulighed for at købe kapacitet i løsningerne. Det sidste ser vi som værende meget relevant i forhold til samkørsel, som af den vej har potentiale til at kunne agere som ”minibusser” i specifikke områder og korridorer.

Samlet set er vi i Nordjylland således meget åbne for de muligheder, som de nye mobilitetsløsninger giver, for at skabe et endnu mere attraktivt mobilitetsudbud for vores kunder.

Når vi kigger på den fremtidige kollektive mobilitet, må vi dog ikke glemme de velfungerende løsninger vi i trafikselskaberne allerede har i dag. Løsninger der er målrettede det mobilitetsbehov vores kunder har. Det være sig i forhold til både pendler- og fritidsrejsende. Løsningerne er de traditionelle kollektive løsninger som bus- og togtrafik,

Nordjyllands Trafikselskab
John F. Kennedys Plads 1T, 3. Sal
9000 Aalborg

Tlf.: +45 9934 1111
Fax: +45 9934 1101
info@NTmail.dk

men også de fleksible behovsstyrede løsninger som ”Plustur” og ”Flextur”. De fleksible behovsstyrede løsninger er en del af den samlede flextrafik i Danmark, som også inkluderer de visitationsbelagte kommunale og regionale kørselsordninger. Ordninger der ikke per definition udføres igennem det regionale trafikselskab, men som udgør en stigende del af den samlede omkostning for det samlede mobilitetsudbud.

(3) Hvad kan din organisation bidrage med i forhold til de kollektive mobilitetsløsninger?

Som mobilitetsselskab forbinder vi ikke bare alle kollektive transportformer i Nordjylland – vores rolle er at sørge for, at det er nemt at komme til og fra arbejde, uddannelse, fornøjelser og hinanden. Vi skaber sammenhænge i både hverdagen og weekenden og bidrager til såvel vækst som trivsel i Nordjylland. Vores rolle er med andre ord at binde Nordjylland sammen. Hos NT arbejder vi desuden målrettet på at skabe et Nordjylland, hvor det er let og enkelt at rejse sammen.

Vi arbejder derfor målrettet med at gøre den kollektive mobilitet i Nordjylland mere sammenhængende, effektiv og målrettet mobilitetsbehovet ved såvel nuværende som potentielle kunder. Det at binde de forskellige kollektive mobilitetsløsninger sammen, er vores rolle som regionalt trafikselskab, og den rolle bør vi også have fremadrettet. Naturligvis i tæt samarbejde med vores ejere, og de mange private mobilitetsaktører vi, allerede i dag, har tætte samarbejdsrelationer med.

Med den beskrevne udvidelse af mobilitetspaletten, med mange nye private mobilitetsformer, vil vores rolle som regionalt trafikselskab, i endnu højere grad, blive en slags broker eller koordinator. Det for at sikre de bedste betingelser for f.eks. mikromobilitet, og samspillet med den øvrige kollektive mobilitet. Det sidste her primært for at bibeholde den helt essentielle sammenhæng i det samlede kollektive mobilitetssystem. Det kræver selvsagt, at rammebetingelserne for vores virke gennemgår et længe tiltrængt servicetjek, så disse er tidssvarende og fyldestgørende.

Med venlig hilsen

Thomas Eybye Øster
Administrerende direktør
Nordjyllands Trafikselskab

Nordjyllands Trafikselskab
John F. Kennedys Plads 1T, 3. Sal
9000 Aalborg

Tlf.: +45 9934 1111
Fax: +45 9934 1101
info@NTmail.dk

9. februar 2024

6. Eventuelt

9. februar 2024

7. Kommende sager

- Godkendelse af Regnskab 2023 til revision
- Status for nuværende forretningsplan og strategiproces 2024
- Driftstatus for Nordjyske Jernbaner A/S, herunder tema om sporspærringer
- Indstilling af eksterne medlemmer til NJ's bestyrelse
- Valg af tilbud, 30.1 udbud af bustrafik

Punkt 8: Beslutningsreferat

9. februar 2024

9. Bestyrelsens 15 min.